# Grupo Aeroportuario, Ferroviario, de Servicios Auxiliares y Conexos Olmeca-Maya-Mexica S.A. de C.V.

---

Metodología para la Administración de Riesgos

# Contenido

Introducción ..... 3

Desarrollo de la Metodología para la Administración de Riesgos ..... 4

Identificación ..... 5

Evaluación ..... 10

Mitigación ..... 21

Monitoreo y comunicación ..... 24

Cédula de Autorizaciones ..... 25

# Introducción

El presente documento muestra de manera general la metodología propuesta para la Administración Integral de Riesgos en el Grupo, la cual se basa en el ACUERDO por el que se emiten las disposiciones y el manual administrativo de aplicación general en materia de control interno, estándares internacionales y buenas prácticas.

La Metodología aplicada es de juicio experto, es por ello por lo que cada Unidad designará a su Líder de Gestión de Riesgo y quien determinará los procesos clave y de apoyo necesarios para cumplir con los objetivos estratégicos.

Sobre los procesos seleccionados, se identificarán los factores de riesgo que amenazan el cumplimiento de los objetivos y metas, así como las medidas de control que se tienen establecidas.

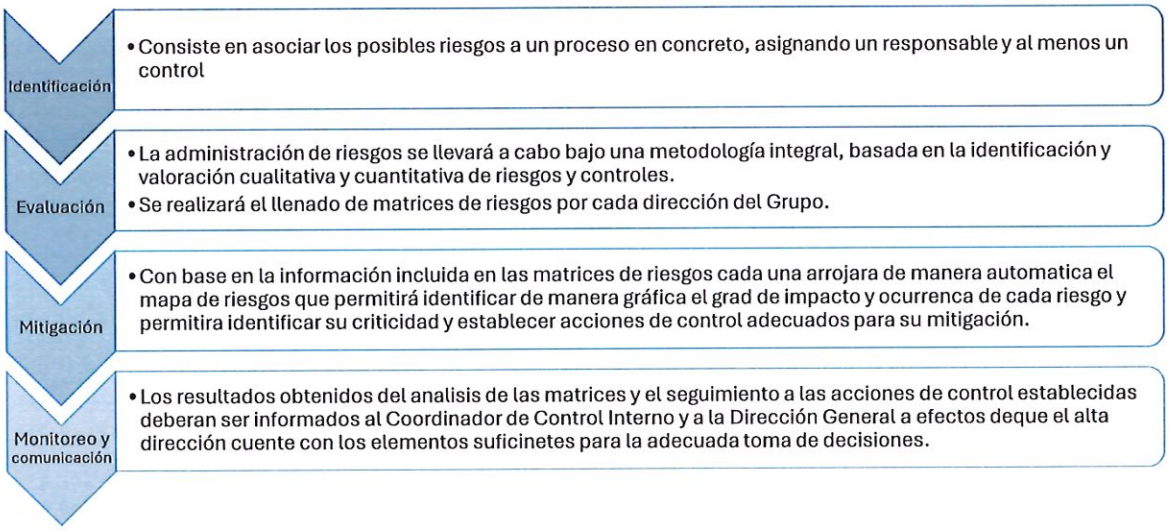
## Desarrollo de la Metodología para la Administración de Riesgos

El Riesgo es la posibilidad de ocurrencia de pérdidas causadas por deficiencias o fallas en los procesos; se refieren a la posibilidad es un evento adverso e incierto (externo o interno) que derivado de la combinación de su probabilidad de ocurrencia y el posible impacto pudieran obstaculizar o impedir el logro de las metas y objetivos institucionales.

Por lo que el Grupo Mundo Maya se encuentra expuesto a diversas circunstancias, causas, o situaciones internas o externas que aumentan la probabilidad que los riesgos se materializasen, por lo que es importante definir las estrategias a seguir para minimizar los impactos. Entre los factores de riesgo se encentran, factores humanos con errores involuntarios, eventos tecnológicos, legales y eventos externos que el Grupo no puede controlar como son desastres naturales.

Otro tipo de riesgos a los que se encuentra expuesto el Grupo son los riesgos de corrupción y reputacionales que podrían considerarse como los que derivan de conductas inapropiadas, irregulares o fraudulentas y provocan alarma, temor o rechazo entre los clientes y se reflejan en la opinión pública de forma negativa y perjudicial para la imagen.

Con base en lo anterior, con el objeto de contar con los elementos que permitan que el Grupo cuente con una adecuada administración de los riesgos dentro de la presente Metodología de se desarrollaran los siguientes cuatro puntos:



# Identificación

El objetivo de la identificación de riesgos es asegurar que se reconozcan todos los riesgos potenciales en el Grupo, y con ello establecer las estrategias para hacer frente a los mismos. Para la identificación de riesgos se deberán seguir los siguientes pasos:

**Paso 1. Generar un inventario de riesgos.**

Se tomarán como base los riegos identificados en ejercicios anteriores, observaciones de auditorías, pérdidas asociadas. De los riesgos identificados se integrará un inventario que deberá ser actualizado al menos una vez al año.

**Paso 2. Generar un inventario de procesos**

Como parte fundamental para la **identificación de los riesgos** en el Grupo se deberá contar con inventario de los procesos del grupo listándolos a manera de inventario señalando si se trata de sustantivos o administrativos. Para coadyuvar a la identificación de riesgos, a la actualización del inventario de riesgos y a la generación del Programa de Trabajo de Control Interno, se aplicarán los siguientes criterios de selección:

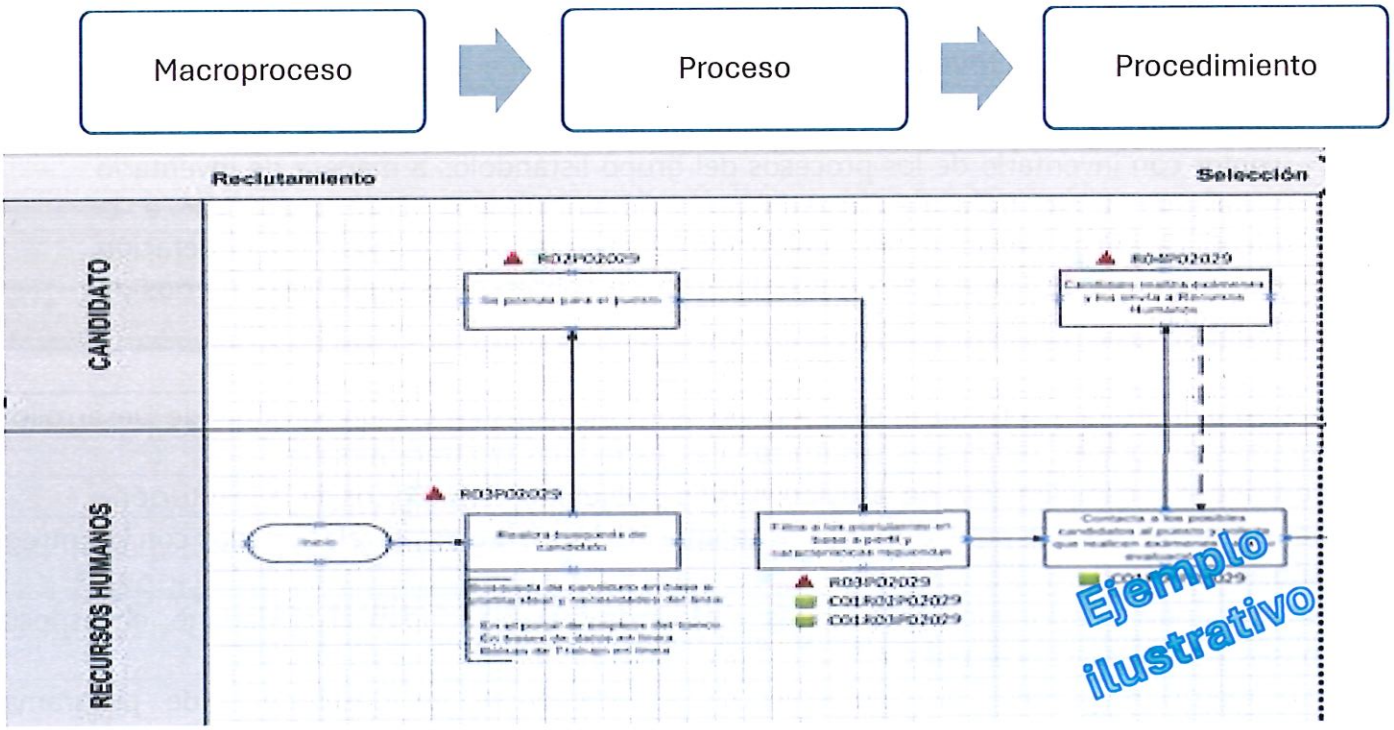
| Criterios |
|---|
| a) Aporta al logro de los compromisos y prioridades incluidas en el Plan Nacional de Desarrollo y programas sectoriales, regionales, institucionales, especiales y/o transversales. |
| b) Contribuye al cumplimiento de la visión, misión y objetivos estratégicos de la Institución. |
| c) Genera beneficios a la población (mayor rentabilidad social) o están relacionados con la entrega de subsidios. |
| d) Se encuentra relacionado con trámites y servicios que se brindan al ciudadano, en especial permisos, licencias y concesiones. |
| e) Su ejecución permite el cumplimiento de indicadores de desempeño de programas presupuestarios o se encuentra directamente relacionado con una Matriz de Indicadores para Resultados. |
| f) Tiene un alto monto de recursos presupuestales asignados. |
| g) Es susceptible de presentar riesgos de actos contrarios a la integridad, en lo específico de corrupción. |
| h) Se ejecuta con apoyo de algún sistema informático. |

**Paso3. Verificar la existencia de flujogramas**

Como parte fundamental para la identificación de los riesgos, se verificará la existencia de flujogramas por proceso o bien en su caso la Dirección de Control del Desempeño Organizacional llevará a cabo el mapeo de los procesos, a través de la Gerencia de Evaluación de Procesos.

El objetivo y principales características del mapeo de procesos es el de identificar y conocer los procesos con mayor exposición al riesgo, entender e identificar cuáles son los principales riesgos del proceso y definir las estrategias para la implementación de controles.

El Mapeo de los procesos debe realizarse desde un enfoque integral, siguiendo el enfoque de lo general a lo particular de acuerdo con la siguiente escala:




**Paso 4. Identificar dentro del programa institucional del Grupo las metas y objetivos**

Una vez integrado el inventario de procesos, se deberán relacionar también con los objetivos y metas de ésta, que se encuentran documentados en el Programa

estratégico del Grupo. asimismo, se deberá revisar el inventario de riesgos existente y en su caso, relacionar los procesos con alguno de los riegos, así como indicar si tienen pérdidas asociadas, e identificar los procesos proclives a riesgos de corrupción.

Con base en lo anterior se obtendrá una base de datos como a continuación se muestra:

Defensa — Inventario de Procesos — Mundo Maya

Ejemplo ilustrativo

| Cve. | Proceso | Tipo Sustantivo /Administrativ | Unidad Responsable (Dueña del | Objetivos de la Unidad responsable | Metas de la unidad responsable | Riesgos asociados | Pérdidas asociadas | Criterios de Selección | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | a) | b) | c) | d) | e) | f) | g) | h) |
| 1 | Implementación [illegible] Clima y Cultura Organizacional y Programa de Prácticas de Trabajo [illegible] | Administrativo | SGAF | | | | | ☐ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ | ☐ |
| 2 | [illegible] Perfil y valuación de puestos | Administrativo | SGAF | | | | | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ | ☒ | ☒ |
| 3 | [illegible] Servicio social y prácticas profesionales | Administrativo | SGAF | | | | | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ |
| 4 | Reclutamiento y selección | Sustantivo | SGAF | | | | | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ | ☒ | ☒ |
| 5 | Resguardo documental | Sustantivo | SGAF | | | | | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ |
| 6 | Nombramiento de servidores públicos y credencialización de personal | Administrativo | SGAF | | | | | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ |
| 7 | Control de plazas y noministas de personal | Administrativo | SGAF | | | | | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ | ☒ | ☒ |
| 8 | Mediación y resolución de conflictos laborales | Sustantivo | SGAF | | | | | ☒ | ☐ | ☐ | ☒ | ☒ | ☒ | ☐ | ☒ |
| 9 | Gestión de terminación de la relación laboral | Sustantivo | SGAF | | | | | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ |
| 10 | Capacitación y sensibilización en derechos laborales | Administrativo | SGAF | | | | | ☐ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ |
| 11 | Gestión de bodas | Administrativo | SGAF | | | | | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ |

## Paso 5. Integrar un Cronograma con las actividades a realizar

El cronograma deberá contener las actividades a realizar designación de responsables y fechas compromiso para la entrega de productos. Este deberá ser autorizado por el Dir. General, Coordinador de Control Interno y Enlace de Admón. de Riesgos.

**GRUPO MUNDO MAYA**
**Cronograma para elaboración de la Matriz de Riesgos Institucional y Programa de Trabajo de Administración de Riesgos (PTAR) 2027**

| Actividad | Ejercicio 2026 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Octubre | | | Noviembre | | | | Diciembre | | |
| | Semana | | | | | | | | | |
| | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 1 | 2 | 3 |
| Instruye a las Unidades, al CCI y al EARI iniciar el proceso de administración de riesgos. | DG | | | | | | | | | |
| Aprueba la metodología de administración de riesgos. | CCI | | | | | | | | | |
| Comunica a las Unidades Administrativas el objetivo del PTAR y la metodología de administración de riesgos | EARI | | | | | | | | | |
| Se solicita a las Unidades se designe un enlace y suplente para la elaboración de la matriz de riesgos. | EARI | | | | | | | | | |
| Se orienta a los enlaces y suplentes de las Unidades sobre el establecimiento de la metodología de administración de riesgos y las acciones para su aplicación. | | EARI | | | | | | | | |
| Documentan los riesgos en la Matriz de Administración de Riesgos. | | Unidades | | | | | | | | |
| Revisa, analiza la información proporcionada por las Unidades y se define la propuesta de PTAR | | | | EARI | | | | | | |
| Elabora y presenta al Coordinador de Control Interno el proyecto del PTAR Institucional. | | | | | | | EARI | | | |
| Revisa y autoriza el proyecto del PTAR Institucional. | | | | | | | | CCI | | |
| Presenta para autorización y firma del Director General la Matriz de Administración de Riesgos, el Mapa de Riesgos y el PTAR. | | | | | | | | | | CCI |
| Firma Matriz de Administración de Riesgos, el Mapa de Riesgos y el PTAR, e instruye a difusión e implementación. | | | | | | | | | | DG |
| Difunde la Matriz de Administración de Riesgos, el Mapa de Riesgos y el PTAR, e instruye la implementación del PTAR a los responsables de las acciones de control comprometidas | | | | | | | | | | CCI |

| Elaboró | Supervisó | Aprobó |
|---|---|---|
| **Enlace de Administración de Riesgos y Dir. Control del Desempeño Org.** | **Subdir. General Corporativo y Coordinador de Control Interno** | **Director General.** |
| **Mtro. Raúl Romero Hernández** | **Mtro. Alejandro Silva Hernández** | **Mtro. Ricardo Flores González** |

| Siglas | Definición |
|---|---|
| DG | Director General |
| CCI | Coordinador de Control Interno |
| EARI | Enlace de Administración de Riesgos Institucional |

**Paso 6. Integrar un Grupo de Trabajo**

Con base en las fechas programadas en el cronograma autorizado por el Director General, Coordinador de Control Interno y Enlace de Administración de Riesgos, se convocará a una reunión a los titulares de cada área del Grupo, con el objeto de establecer un Grupo de Trabajo para el adecuado análisis de los riesgos y fomentar la cultura de la Administración de estos, incluyendo la el llenado de las matrices, designación de responsables o líderes de Gestión de Riesgos (titular y suplente), el perfil del mismo y llevar a cabo la presentación del cronograma para realizar el PTAR.

**Paso 7. Designación de Responsables. (Líderes de Gestión de Riesgos)**

Durante la reunión para la integración del Grupo de Trabajo, se solicitará a cada una de las Direcciones del Grupo que designen a un representante quien fungirá como líder de gestión de riesgos, quien será el responsable de la identificación de Riesgos, llenado de la Matriz de Riesgos y controles y seguimiento a las acciones de control resultantes de esta actividad.

La Persona Servidora Pública designada como responsable o líder de Gestión de Riesgos deberá cumplir con las siguientes características:

1. Tener nivel mínimo de Jefe de Departamento.
2. Contar con capacidad para la toma de decisiones sobre la Dirección que represente.
3. Conocer la totalidad de las actividades, procedimientos, procesos, objetivos y metas de la Dirección que representa.

**Paso 8. Elaboración de contexto**

El Enlace de Administración de Riesgos deberá:

1. Describir y documentar el entorno externo social, político, legal, financiero, tecnológico, económico, ambiental y de competitividad de la institución.
2. Describir las situaciones intrínsecas al Grupo relacionadas con su estructura, atribuciones, procesos, objetivos y estrategias, recursos humanos, materiales y financieros, programas presupuestarios y la evaluación de su desempeño, así como su capacidad tecnológica bajo las cuales se puedan identificar sus fortalezas y debilidades para responder a los riesgos que sean identificados.
3. Identificar, seleccionar y agrupar los enunciados definidos como supuestos en los procesos del Grupo a fin de contar con un conjunto sistemático de eventos adversos de realización incierta que puedan afectar el cumplimiento de los objetivos.

4. Describir el comportamiento histórico de los riesgos identificados en ejercicios anteriores, tanto lo relativo a su incidencia efectiva como en el impacto que, en su caso, hayan tenido sobre el logro de los objetivos institucionales.

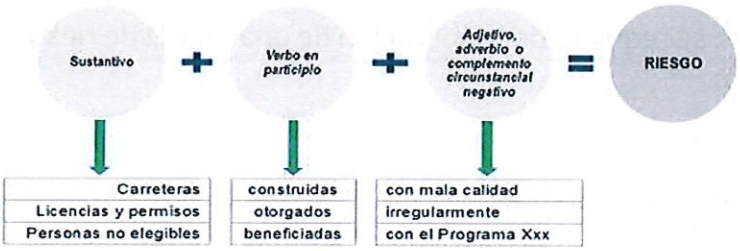
**Paso 9. Herramientas para la identificación de riesgos**

El personal de la Dirección de Control del Desempeño Organizacional realizará un acompañamiento en la identificación de riesgos teniendo como fuentes la siguientes:

- Entrevistas directas con los Líderes de Gestión de Riesgo.
- Notificaciones por parte de las áreas de la presentación de un evento de Riesgo Operacional mediante los canales destinados para tales efectos.
- Informes y hallazgos de auditoría, supervisiones o revisiones.
- Inventario de riesgos.
- Contexto de la Institución.

La identificación de riesgos se encuentra sustentado en aproximaciones a través de la opinión de los expertos del Grupo es decir de los Gestores de Riesgo (cualitativo) y registros de las pérdidas ocurridas (cuantitativo).

La redacción de los riesgos deberá seguir la siguiente estructura:




Y una vez redactados se incluirán en la matriz de identificación de riesgos como se describe en el apartado II. Evaluación.

# Evaluación

La evaluación refiere al proceso de medir qué tan probable y qué tan grave sería cada riesgo, para decidir dónde actuar primero, permite priorizar riesgos, asignar recursos, elegir la respuesta, definir responsables, plazos e indicadores de seguimiento.

**Paso 1. Llenado de matrices de riesgos**

Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades más importantes de la entidad, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos (factores de riesgo), permite evaluar la efectividad de una adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende al logro de los objetivos de la organización. La matriz de riesgos tiene como finalidad, establecer las bases para la valoración de los riesgos respecto a los controles.

Para lo anterior, se requiere de la aplicación de una matriz de riesgos integral en la cual se identifiquen:

- Riesgos
- Controles asociados
- Planes de Acción
- Indicadores asociados a procesos, riesgos y/o controles
- Proporcionan una estimación cuantitativa obtenida de los responsables de los procesos y podrá ser complementado por los datos recogidos en las BD de pérdidas de la institución.

Las matrices cuentan con una serie de campos cuyo llenado se realizar con base en lo siguiente:

a. **Ramo / sector:** Seleccionar el ramo administrativo o sector al que pertenece el Grupo.

b. **Institución:** Incorporar el nombre de la dependencia, órgano administrativo desconcentrado, o entidad de la APF, de que se trate.

c. **Año:** Anotar a cuatro dígitos el año en el que se integra la matriz de riesgos.

d. **Titular de la institución:** registrar el nombre del Director General del Grupo, quien aprobará con su firma autógrafa la Matriz de Administración de Riesgos.

e. **Coordinador de control interno:** Registrar el nombre del Coordinador de Control interno designado por el Titular de la Institución, para coordinar y supervisar el proceso de Administración de Riesgos.

f. **Enlace de administración de Riesgos:** Registrar el nombre del Enlace de Administración de Riesgos designado por el Coordinador de Control Interno, para la integración e incorporación en el Sistema informático del proceso de administración de Riesgos.

g. **Número de riesgo:** se visualizará de manera automática y de forma consecutiva una vez ingresados los datos anteriores. La estructura del número de riesgo se construirá con el año de captura del mismo y el número consecutivo asignado por el Grupo.

h. **Unidad administrativa:** la unidad administrativa responsable de administrar el riesgo identificado.

i. **Estrategia, objetivo o meta:** describir brevemente la estrategia, objetivo, meta o el proceso prioritario al que este alineado el riesgo identificado según corresponda.

j. **Riesgo:** Registrar el nombre y la descripción del riesgo identificado por el líder de Gestión de Riesgos en acompañamiento con el Enlace de Administración de Riesgos.

k. **Nivel de decisión del riesgo:** identificar el nivel de exposición del riesgo en caso de su materialización: estratégico, directivo u operativo.

- Estratégico: que el nivel de exposición del riesgo sea "estratégico" significa que, si el riesgo se materializa, sus consecuencias rebasan un área o proceso y amenazan objetivos institucionales de alto nivel (misión, metas del plan, compromisos regulatorios clave, reputación y continuidad), requiriendo decisiones de alta dirección/órganos de gobierno y ajustes a la estrategia o al presupuesto.

- Directivo: que el nivel de exposición sea directivo significa que, si el riesgo llega a materializarse, el impacto rebasa la esfera operativa/gerencial y compromete objetivos estratégicos, cumplimiento de alto nivel, reputación institucional o continuidad de servicios críticos, por lo que exige decisiones e intervención inmediata de la dirección.
- Operativo: si el riesgo ocurre, el daño principal se manifiesta en la operación diaria: procesos, servicios, tiempos de ciclo, calidad, capacidad y continuidad. Es decir, afecta el "cómo" se ejecuta el trabajo, más que generar de inmediato sanciones legales, pérdidas financieras directas o daño reputacional.

I. **Clasificación del riesgo:** Seleccionar el tipo de riesgo, en congruencia con la descripción de este;

- Sustantivo: riesgos que afectan la misión principal de la institución.
- Administrativo: problemas en funciones de apoyo interno (trámites, archivos, compras, control documental).
- Legal: incumplir leyes, contratos o regulaciones y recibir sanciones.
- Financiero: pérdidas de dinero o distorsión de cifras por errores, fraudes, tipo de cambio o mercado.
- Presupuestal: fallas en programar, autorizar o ejercer el presupuesto.
- Servicios: bajar la calidad o interrumpir la prestación al público/usuarios internos.
- Seguridad: daños a personas, instalaciones o bienes (física y patrimonial).
- Obra pública: riesgos en planeación, contratación, ejecución o calidad de obras.
- Recursos humanos: dotación, selección, capacitación, clima laboral y rotación.
- Imagen (reputacional): pérdida de confianza pública por hechos, omisiones o comunicación deficiente
- Tic's: caídas de sistemas, ciberataques, pérdida de datos, baja disponibilidad
- Salud: afectaciones a la salud de personal o usuarios (condiciones, contagios, emergencias).
- Corrupción: uso indebido del cargo para beneficio propio o de terceros (sobornos, desvíos, conflicto de interés).
- Otros. Se deberá registrar el tipo de riesgo que corresponde en la columna adjunta a la derecha, considerando que no sea de naturaleza similar a las opciones indicadas. En caso de elegir otros se deberá registrar el tipo de riesgo.

m. **Factor:** describir la circunstancia, causa o situación interna y/o externa que aumenta la probabilidad de que un riesgo se materialice. Se podrán incorporar como máximo cinco factores.

**Clasificación de factores:**

- Humano: se relacionan con las personas (internas o externas), que participan directa o indirectamente en los programas, proyectos, procesos, actividades o tareas.
- Financiero presupuestal: se refieren a los recursos financieros y presupuestales necesarios para el logro de metas y objetivos.
- Técnico-administrativo: se vinculan con la estructura orgánica funcional, políticas, sistemas no informáticos, procedimientos, comunicación e información, que intervienen en la consecución de las metas y objetivos.
- Tic's: se relacionan con los sistemas de información y comunicación automatizados.
- Material: se refieren a la infraestructura y recursos materiales necesarios para el logro de las metas y objetivos.
- Normativo: se vinculan con las leyes, reglamentos, normas y disposiciones que rigen la actuación de la organización en la consecución de las metas y objetivos.
- Entorno: se refieren a las condiciones externas a la organización, que pueden incidir en el logro de las metas y objetivos.

**Tipo de factores**

- Interno: se encuentra relacionado con las causas o situaciones originales en el ámbito de la organización.
- Externo: Se refiere a las causas o situaciones fuera del ámbito de competencia de la organización.

n. **Posibles efectos del riesgo:** describir las consecuencias que incidirán en el cumplimiento de las metas y objetivos institucionales, en caso de materializarse en el riesgo identificado.

o. **Valoración Inicial:** Se determinará sin considerar los controles existentes para administrar los riesgos, a fin de visualizar la máxima vulnerabilidad a que está expuesta la Institución de no responder ante ellos adecuadamente

p. **Grado de Impacto**: La asignación se determinará con un valor del 1 al 10 en función de los efectos, de acuerdo con la siguiente escala de valor.

| Escala de valor | Impacto | Descripción |
|---|---|---|
| 10 | Catastrófico | Influye directamente en el cumplimiento de la misión, visión, metas y objetivos de la Institución y puede implicar pérdida patrimonial, incumplimientos normativos, problemas operativos o impacto ambiental y deterioro de la imagen, dejando además sin funcionar totalmente o por un período importante de tiempo, afectando los programas, proyectos, procesos o servicios sustantivos de la Institución. |
| 9 | | |
| 8 | Grave | Dañaría significativamente el patrimonio, incumplimientos normativos, problemas operativos o de impacto ambiental y deterioro d la imagen o logro de las metas y objetivos institucionales. Además se requiere una cantidad importante de tiempo para investigar y corregir los daños. |
| 7 | | |
| 6 | Moderado | Causaría, ya sea una pérdida importante en el patrimonio o un deterioro significativo en la imagen institucional. |
| 5 | | |
| 4 | Bajo | Causa un daño en el patrimonio o imagen institucional, que se puede corregir en el corto tiempo y no afecta el cumplimiento de las metas y objetivoos institucionales. |
| 3 | | |
| 2 | Menor | Riesgo que puede ocasional pequeños o nulos efectos en la Institución. |
| 1 | | |

q. **Probabilidad de ocurrencia:** La asignación se determinará con un valor del 1 al 10, en función de los factores de riesgo, considerando las siguientes escalas de valor.

Para realizar una evaluación efectiva es necesario que se conozcan los siguientes elementos:

| Escala de valor | Probabilidad de ocurrencia | Descripción |
|---|---|---|
| 10 | Recurrente | Probabilidad de ocurrencia muy alta.<br>Se tiene la seguridad de que el riesgo se materialice, tiende a estar entre 90 % y 100% |
| 9 | | |
| 8 | Muy probable | Probabilidad de ocurrencia alta.<br>Está entre 75% a 89% la seguridad de que se materialice el riesgo. |
| 7 | | |
| 6 | Probable | Probabilidad de ocurrencia media.<br>Está entre 51% a 74% la seguridad de que se materialice el riesgo. |
| 5 | | |
| 4 | Inusual | Probabilidad de ocurrencia baja.<br>Está entre 25% a 50% la seguridad de que se materialice el riesgo. |
| 3 | | |
| 2 | Remota | Probabilidad de ocurrencia muy baja.<br>Está entre 1% a 24% la seguridad de que se materialice el riesgo. |
| 1 | | |

a. Riesgo Inherente

El riesgo inherente se define como el nivel de riesgo propio de la actividad, por lo que la medición de este resulta compleja, y los valores de frecuencia y severidad pueden resultar extremos debido a que en un escenario de **ausencia total de controles o mitigantes**, la materialización del riesgo se puede dar en todos los eventos con un impacto económico total.

b. Controles

Es una medida (política, procedimiento, actividad o herramienta) diseñada para reducir la probabilidad y/o el impacto de un riesgo y dar seguridad de cumplir objetivos del Grupo.

Lo esencial de un control:

1. Propósito: qué riesgo mitiga y qué objetivo protege.
2. Dueño: quién lo ejecuta y quién lo supervisa.
3. Qué y cómo: la actividad concreta, criterio/umbral y la herramienta usada.
4. Cuando y con qué frecuencia: momento en el proceso (ex-ante/ex-post) y periodicidad.
5. Evidencia: rastro verificable (documento, registro, log, acta, reporte).

c. Riesgo Residual

Se refiere a la valoración de frecuencia y severidad después de la aplicación de los controles. Para la evaluación de los Riesgos se realiza a **juicio experto** que se refiere a que el Gestor de Riesgos documenta basado en su experiencia la probabilidad de ocurrencia e impacto, en caso de materializarse cada riesgo para obtener la escala de riesgo inherente.

## 2. Evaluación de Controles

### 2.1 Suficiencia y deficiencia

Para realizar la evaluación de controles se deberán comprobar la existencia de estos para cada uno de los riesgos identificados, (documentando en la matriz de riesgos 5 como máximo por cada riesgo) describirlos y determinar el tipo de control, especificando si es:

- Preventivo: Un control preventivo es una medida que se ejecuta antes de que ocurra el evento no deseado para evitar que el riesgo se materialice (o reducir al mínimo su probabilidad). Actúa sobre causas o condiciones del riesgo, no sobre las consecuencias.
- Correctivo: Un control correctivo es una medida que actúa después de que se detecta una desviación, error o incidente. Su propósito es contener el daño, revertirlo (en lo posible), restaurar la operación y evitar la reincidencia mediante acciones de remediación y aprendizaje.
- Detectivo: Un control detectivo es una medida que no evita que ocurra el evento, sino que lo identifica oportunamente (o sus señales) para avisar, registrar y detonar corrección. Actúa después o casi en tiempo real y busca acotar la duración/alcance del impacto y generar evidencia.

Una vez realizado lo anterior se identificará la suficiencia o deficiencia. Considerando para tales efectos que un control será deficiente si **no** cumple alguna de las siguientes condiciones:

- Está documentado: se encuentra descrito
- Esta formalizado: se encuentra autorizado por un servidor público facultado, de acuerdo con los lineamientos establecidos por el propio Grupo Mundo Maya.
- Se aplica: se ejecuta consistentemente el control.
- Es efectivo: cuando se incide en el factor del riesgo, es decir que causa un efecto favorable que permite disminuir la probabilidad de ocurrencia del riesgo.

Por ende, un control será suficiente cuando se cumplan todos los requisitos anteriores, en ese orden de ideas, si un riesgo cuenta con al menos un control evaluado como deficiente, se considera que no se encuentra controlado, por lo que el impacto y probabilidad de ocurrencia permanecerán en con sus impactos originales, es decir mantiene su riesgo inherente. Los resultados permitirán observar, en términos cualitativos, qué tan efectivos son los controles y qué planes de mejora se pueden ejecutar.

Por el contrario, si el total de los controles se consideran **suficientes**, el riesgo deberá modificarse en su probabilidad de ocurrencia y/o grado de impacto a uno menor. Es decir, cambia de riesgo inherente a riesgo residual.

### 2.2 Efectividad y nivel de ejecución

Adicional a lo anterior, los controles deberán ser evaluados de acuerdo con dos características: efectividad y nivel de ejecución, de conformidad con lo siguiente:

**Efectividad,** se refiere a que cuando un control es aplicado permite disminuir la probabilidad de ocurrencia, es decir, se refiere a la reducción del nivel de exposición al riesgo y está relacionada de forma inversa con el impacto, a mayor efectividad menor impacto.

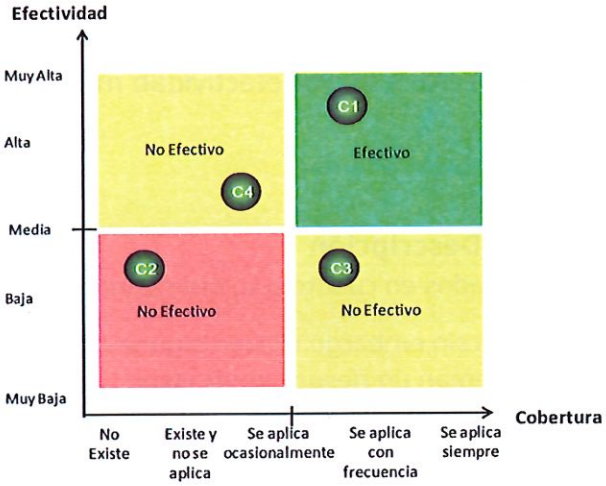
| Escala | Definición | Descripción |
|---|---|---|
| 3 | Fuerte | Los controles son adecuados en cuanto a su diseño inherente. |
| 2 | Moderada | Los controles son adecuados sin embargo existen algunas debilidades que no representan un riesgo significativo. |
| 1 | Débil | Los controles no son de nivel aceptable. |

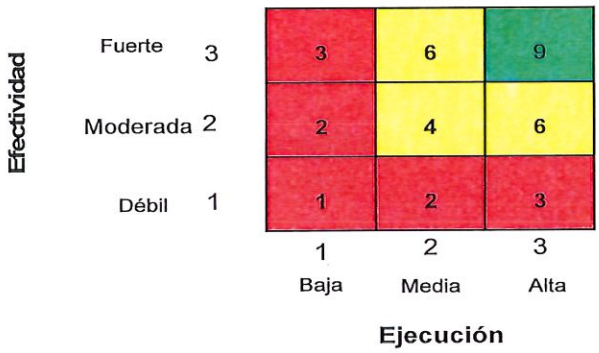
**Ejecución** refiere a que los responsables del control lo ejecutan y se cuenta con evidencia de que el control es aplicado consistentemente. Refiere a la frecuencia con el que se llevan a cabo los controles ya que parte fundamental de la disminución de riesgo le corresponde a la aplicación periódica estos.

En tal sentido la ejecución se encuentra asociada a un nivel de probabilidad, si la ejecución es alta entonces la probabilidad de que ocurra un evento es menor, es decir, tienen una relación inversa.

| Escala | Definición | Descripción |
|---|---|---|
| 3 | Alta | El control se aplica de la forma planeada, en cuanto a periodicidad establecida y dueños del control asignados. |
| 2 | Media | El control tiene algunas fallas en su aplicación, sin embargo, no representa mayores riesgos. |
| 1 | Baja | El control no se aplica de la forma planeada en cuanto a su ejecución y/o ejecutor poniendo en riesgo el cumplimiento de su objetivo. |

Una vez que se han evaluado los controles, la metodología considera que dependiendo de la calificación de los controles se reducirá el riesgo. Derivado de lo anterior se aplica una matriz con la finalidad de evaluar cuán importante es cada control para un riesgo:

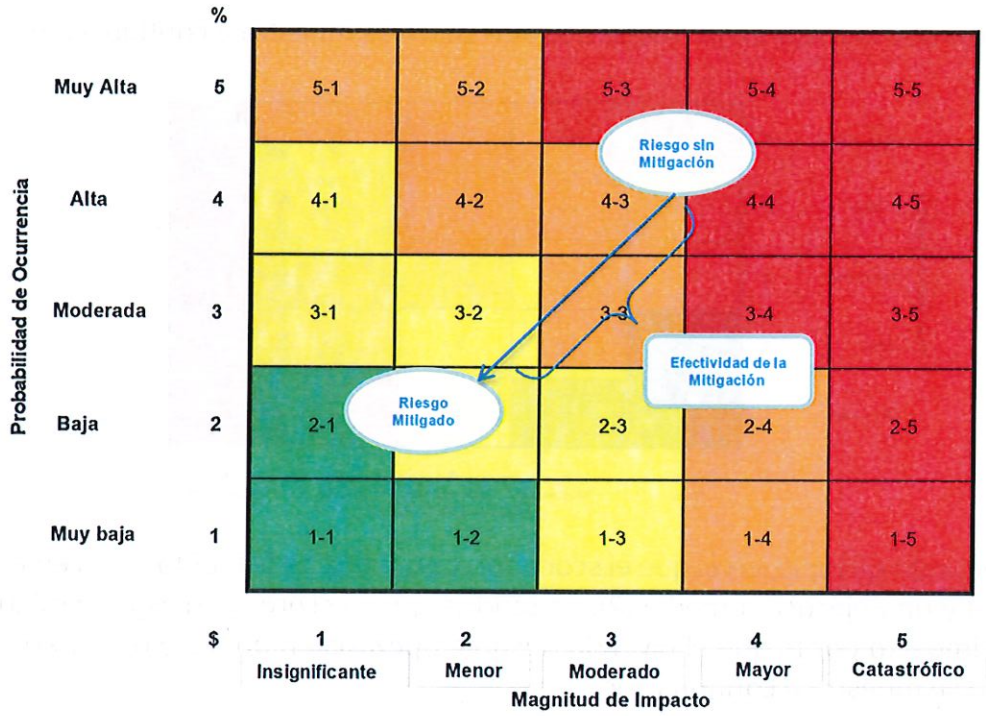



Es importante destacar que, únicamente los controles evaluados con una solidez "Fuerte" (color verde) o "Moderada" (color amarillo), pueden mejorar la calificación del riesgo, ya sea de probabilidad de ocurrencia o de magnitud de impacto, dependiendo del tipo de control, de conformidad con la siguiente tabla:

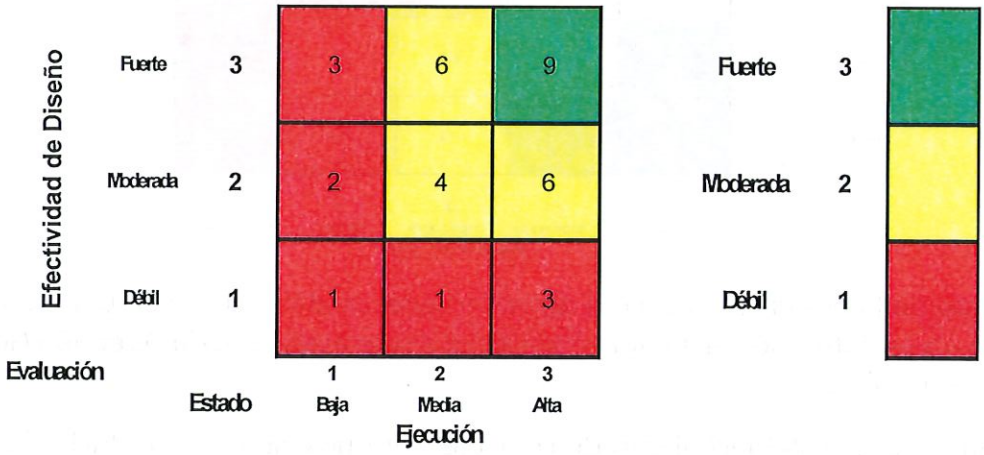
| Efectividad / Ejecución | Reducción en Niveles de Probabilidad | Reducción en Niveles de Impacto |
|---|---|---|
| 3,3 | -1 | -1 |
| 3,2 | 0 | -1 |
| 3,1 | 0 | 0 |
| 2,3 | -1 | 0 |
| 2,2 | -1 | 0 |
| 2,1 | 0 | 0 |
| 1,3 | 0 | 0 |
| 1,2 | 0 | 0 |
| 1,1 | 0 | 0 |

Es así como después de la aplicación de controles se obtiene el **Riesgo Residual** = (Probabilidad x Impacto), cuando estos son evaluados como suficientes, efectivos y que se ejecutan de manera correcta.



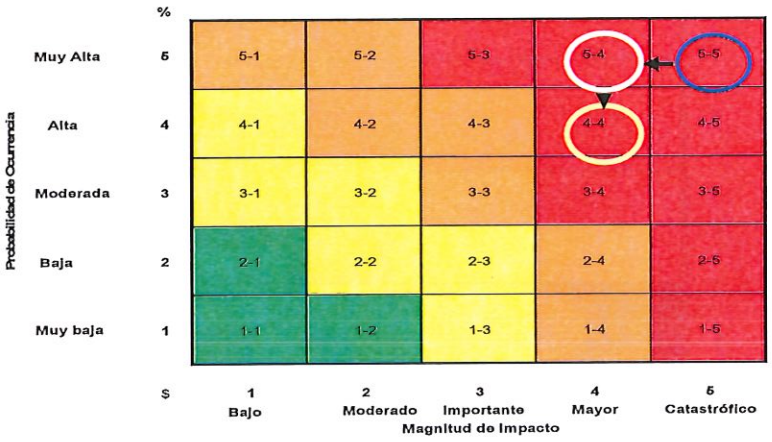

A efecto de clarificar lo descrito, a modo de ejemplo, se tiene que un control efectivo (3), con una ejecución alta (3), tendrá un score de 9 como se muestra en la siguiente matriz

**Solidez del control.**

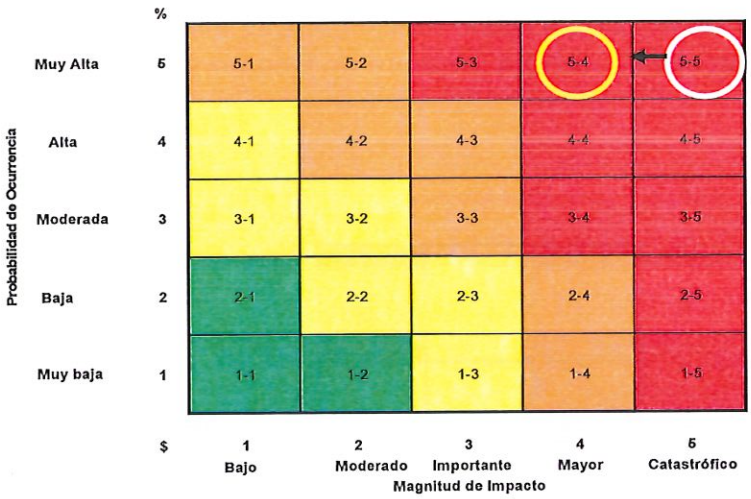



En consecuencia, en la matriz de riesgos se presenta una disminución en un nivel de impacto y en uno de probabilidad, considerando un ejemplo de un riesgo que obtuvo una evaluación de 5 en probabilidad con 5 de impacto, si se le aplica ese control disminuye a 4-4 disminuyendo, obteniendo con ello el score de Riesgo Residual.

Mismo que se mostrara en un mapa de calor como se muestra a continuación




En un segundo ejemplo, en el que el score del control sea de 6 debido a una efectividad fuerte (3) y una ejecución media (2), se tendría que el score de riesgo disminuye un nivel de impacto por lo que el nivel de riesgo empezaría en un 5-5 y terminaría en un 5-4 como se muestra a continuación.




El resultado de la evaluación descrita anteriormente se documenta en una matriz de riesgos, para ser integrada en un informe ejecutivo y presentada a la Dirección General y a los involucrados.

Es así como con el establecimiento de controles internos, se busca reducir el Riesgo Inherente, obteniendo con ello una medida de Riesgo Residual que refleje la migración de los riesgos hacia zonas con una menor probabilidad de ocurrencia, grado de impacto o ambos.

# Mitigación

La mitigación de los riesgos se refiere a las estrategias y acciones diseñadas a abordar los riesgos potenciales que pueda afectar al Grupo, el objetivo es el de minimizar el impacto negativo de estos y asegurar la continuidad de negocios.

**Paso 1. Establecimiento de estrategias**

El objetivo es el establecer sinergias de mejora enfocados a mitigar y/o reducir los riesgos identificados.

Las estrategias se establecerán de acuerdo con lo siguiente:

- **Evitar el riesgo:** se refiere a eliminar el factor o factores que pueden provocar la materialización del riesgo.
- **Reducir el riesgo:** Implica establecer acciones dirigidas a disminuir la probabilidad de ocurrencia y el impacto.
- **Asumir el riesgo**: solo aplicará cuando el riesgo se encuentre en un cuadrante de baja probabilidad d ocurrencia y grado de impacto, o cuando no se tiene opción para abatirlo y sólo pueden establecerse acciones de contingencia.
- **Transferir el riesgo**: consiste en trasladar el riesgo a un externo a través de la contratación de servicios tercerizados, con alguno de los siguientes métodos: (1) Protección o cobertura, cuando la acción que se realiza para reducir la exposición al riesgo obliga también a renunciar a la posibilidad de una ganancia; (2) aseguramiento, significa pagar una prima para que, en caso de pérdidas, éstas sean asumidas por la aseguradora; (3) Diversificación, tomar diferentes estrategias de inversión para reducir la exposición al riesgo.
- **Compartir el riesgo:** distribuir parcialmente el riesgo a diferentes unidades administrativas desde el ámbito de su competencia.

**Paso 2. Planes de Mitigación**

Para mayor detalle y seguimiento de los riesgos y controles identificados y contenidos en la Matriz de Riesgos, será responsabilidad de Las Unidades de Negocio a través del

Líder de Gestión de Riesgo operacional, proponer e implantar los planes de acción en su ámbito de competencia, dichos planes podrán estar vinculados a:

- Riesgos carentes de controles,
- Controles evaluados con efectividad y/o eficiencia baja o nula,
- Procesos que requieran de mejoras o fortalecimiento en sus medidas.

y se priorizarán de acuerdo con lo siguiente:

- Por la severidad del riesgo mitigado,
- Por la facilidad de implantación,
- Por el plazo de implementación,
- Costo de la implementación.

Con base en lo anterior se deberá integrar una base que permita el registro y seguimiento de cada estrategia establecida como plan de mitigación, con base en el

| III – PLAN DE ACCIÓN | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| No. Acción | Riesgo / control / Proceso Asociado | Tipo de Estrategia | | Acciones | Responsable de la acción | Áreas Involucradas | Fecha Inicio | Fecha Término | Costo de Implementación | Tiempo de Implementació |
| 01 | XXXX | Asumir | ● | XXXX | XXXX | XXXX | XX/XX/XX | XX/XX/XX | - | - |

| Bitácora de Seguimiento | | |
|---|---|---|
| Fecha | Actividad | Evidencia |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

siguiente formato:

**Paso 3. Acciones para realizar por el Líder de Gestión de Riesgo**

- Proponer de acuerdo con lo anterior los planes de Mitigación / acción necesarios para los riesgos identificados, controles que requieran de mejoras, o bien proceso en general,
- Coadyuvar a la correcta implementación de los planes de mitigación / acción, mediante el seguimiento, comunicación y monitoreo de los avances, mejoras o cambios que presenten dichos planes.
- Cada Líder de Gestión de Riesgo operacional será el responsable de la implementación de los planes de mitigación / acción.
- Realizar un análisis sobre el costo – beneficio de la implementación de los planes de mitigación / acción.

**Procedimiento para la implementación y seguimiento de planes de acción**

| Paso | Responsable | Acción |
|---|---|---|
| 1 | Enlace de administración de Riesgos | ¿Cuenta con matriz de riesgos?<br>Sí, Continua en la actividad 2<br>No, se deberá realizar la matriz de riesgos |
| 2 | Enlace de administración de Riesgos | ¿La matriz se encuentra actualizada?<br>Sí, Continua en la actividad 3<br>No, se deberá actualizar la matriz de riesgos |
| 3 | Enlace de administración de Riesgos y Líder de Gestión de Riesgos | Identificar los riesgos, controles o bien definir si el proceso requiere asociarse a un plan de mitigación |
| 4 | Enlace de administración de Riesgos y Líder de Gestión de Riesgos | Registrar el plan de mitigación en el formato "Planes de acción" |
| 5 | Enlace de administración de Riesgos y Líder de Gestión de Riesgos | Establecer reuniones periódicas de acuerdo con el tratamiento de cada plan para dar el seguimiento a la implementación de este |
| 6 | Enlace de administración de Riesgos y Líder de Gestión de Riesgos | Reportar avances al Comité de Control de Desempeño Institucional |
| 7 | Enlace de administración de Riesgos y Líder de Gestión de Riesgos | Una vez concluido e implementado el plan de mitigación se dará seguimiento d acuerdo al tratamiento de los controles |

# Monitoreo y comunicación

## 1. Comunicación

Los resultados obtenidos deberán ser informados al Coordinador de Control Interno y la Dirección General a efectos de que la alta dirección cuente con los elementos suficientes para la adecuada toma de decisiones.

Así mismo, el Enlace de Administración de Riesgos del Grupo Mundo Maya divulgará y revelará la información de Riesgos al Comité de Control de Desempeño Institucional y a las diferentes Unidades de Negocio, de manera periódica

## 2. Monitoreo

El monitoreo se refiere a mantener continuamente supervisados los controles implementados, así como a los planes de mitigación para comprobar su efectividad.