

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

INTRODUCCION

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

Todos los servidores públicos, en cumplimiento de sus funciones, estamos sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, este documento tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

DEFINICIONES:

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso, es decir, es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

- **Riesgo institucional:** Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:
 - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
 - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
 - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
 - Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción serán considerados como riesgos de tipo institucional.
- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificados.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

- **Materialización del riesgo:** ocurrencia del riesgo identificado
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar, compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

OBJETIVO GENERAL

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

OBJETIVOS ESPECIFICOS

- Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad estableciendo una metodología para la administración y gestión de los riesgos con actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo adoptando buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

POLITICA DE ADMINISTRACION DEL RIESGO

La Contraloría del Valle del Cauca, adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

1. Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
2. Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

3. Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
4. Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
5. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, el plan forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo

CLASIFICACION DE LOS RIESGOS

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riesgo mediante la definición de controles y planes de manejo:

| Clases de riesgo | Definición |
|------------------|---|
| Estratégico | Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia. |
| Operativo | Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias. |
| Financieros | Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes. |
| Cumplimiento | Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad. |

| | |
|------------|--|
| Tecnología | Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión. |
| Imagen | Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad. |

ANALISIS DE LOS RIESGOS

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

1. CALIFICACIÓN DEL RIESGO

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos.

Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

| Escala para calificar la probabilidad del riesgo | | |
|--|---|--|
| Nivel | Concepto | Frecuencia |
| Raro | El evento puede ocurrir solo en circunstancias excepcionales. | No se ha presentado en los últimos 5 años. |
| Improbable | El evento puede ocurrir en algún momento. | Al menos de 1 vez en los últimos 5 años. |
| Moderado | El evento podría ocurrir en algún momento. | Al menos de 1 vez en los últimos 2 años. |
| Probable | El evento probablemente ocurrirá en la mayoría de las circunstancias. | Al menos de 1 vez en el último año. |
| Casi certeza | Se espera que el evento ocurra en la mayoría de las circunstancias. | Más de 1 vez al año. |

| Escala para calificar el impacto del riesgo | | | | | | | |
|---|---|---|--|--|---|--|--|
| Tipos de efecto o impacto | | a) Estratégico | b) Operativo | c) Financieros | d) Cumplimiento | e) Tecnología | f) Imagen |
| INSIGNIFICANTE | Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución | Afecta el cumplimiento de algunas actividades | Genera ajustes a una actividad concreta | La pérdida financiera no afecta la operación normal de la institución | Genera un requerimiento | Afecta a una persona o una actividad del proceso | Afecta a un grupo de servidores del proceso |
| MENOR | Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución | Afecta el cumplimiento de las metas del proceso | Genera ajustes en los procedimientos | La pérdida financiera afecta algunos servicios administrativos de la institución | Genera investigaciones disciplinarias, y/o fiscales y/o penales | Afecta el proceso | Afecta a los servidores del proceso |
| MODERADO | Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución | Afecta el cumplimiento de las metas de un grupo de procesos | Genera ajustes o cambios en los procesos | La pérdida financiera afecta considerablemente la prestación del servicio | Genera interrupciones en la prestación del bien o servicio | Afecta varios procesos de la institución | Afecta a todos los servidores de la institución |
| MAYOR | Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución | Afecta el cumplimiento de las metas de la institución | Genera intermitencia en el servicio | La pérdida financiera afecta considerablemente el presupuesto de la institución | Genera sanciones | Afecta a toda la entidad | Afecta el sector |
| CATASTRÓFICO | Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución | Afecta el cumplimiento de las metas del sector y del gobierno | Genera paro total de la institución | Afecta al presupuesto de otras entidades o a de la del departamento | Genera cierre definitivo de la institución | Afecta al Departamento | Afecta al Departamento, Gobierno, Todos los usuarios de la institución |

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (Estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

2. EVALUACIÓN DEL RIESGO

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

| PROBABILIDAD | IMPACTO | | | | |
|--------------|----------------|-------|----------|-------|--------------|
| | Insignificante | Menor | Moderado | Mayor | Catastrófico |
| Raro | B | B | B | M | M |
| Improbable | B | M | M | A | A |
| Moderado | B | M | A | A | E |
| Probable | M | A | A | E | E |
| Casi certeza | M | A | E | E | E |

| Color | Zona de riesgo |
|-------|-------------------------|
| B | Zona de riesgo baja |
| M | Zona de riesgo moderada |
| A | Zona de riesgo alta |
| E | Zona de riesgo extrema |

Con la evaluación del riesgo, previa a la formulación de controles se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina **evaluación del riesgo inherente**.

IDENTIFICACIÓN DE CONTROLES

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan las características mínimas que se deben tener en cuenta para la definición de los controles:

| Característica | Descripción |
|-----------------------|--|
| Objetivos | No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener |
| Pertinentes | Están directamente orientados a atacar las causas o consecuencias del riesgo |
| Realizables | Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo |
| Medibles | Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad |
| Periódicos | Tienen frecuencia de aplicación en el tiempo |
| Efectivos | Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo |
| Asignables | tienen responsables definidos para su ejecución |

En el siguiente ejemplo se presenta una forma de redacción de un control.

| Causa | Riesgo | Efecto/Consecuencia | Control |
|--|---------------------------------------|--|---|
| Uso de un calendario tributario obsoleto | Declaración de impuestos extemporánea | Sanciones pecuniarias para la entidad o disciplinaria para un(os) funcionario(s) | El contador y/o el Subdirector Administrativo y Financiero debe realizar la actualización u divulgación, en enero de cada año, de los calendarios tributarios nacionales y departamentales, en la página web, intranet, físicos, etc. |

En esta etapa se deben describir todos los controles, existentes y por definir, deben estar orientados a atacar las causas y/o consecuencias (mitigar y/o eliminar) del riesgo. Una vez se hayan identificado y descrito los controles se debe determinar la clase del control; un control puede ser de tipo preventivo o correctivo como se presenta a continuación:

| Clases de controles | |
|--|--|
| PREVENTIVO | CORRECTIVO |
| Acción o Conjunto de acciones que elimina o mitiga las causas del riesgo | Acción o conjunto de acciones que eliminan o mitigan las consecuencias |
| Orientación a disminuir la probabilidad de ocurrencia del riesgo | Orienta a disminuir el nivel de impacto del riesgo |

Descripción de las clases de controles

EVALUACIÓN DE LOS CONTROLES

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad de la siguiente manera:

| | | |
|---|--------------------------------|--|
| ¿El control está documentado, incluye el responsable y la frecuencia de aplicación? | ¿El control se está aplicando? | ¿El control es efectivo (sirve o cumple su función)? |
|---|--------------------------------|--|

- Si la pregunta relacionada con documentación se está cumpliendo, se deben asignar 25 puntos; en caso contrario marque 0.
- Si la pregunta relacionada con aplicación se está cumpliendo, se deben asignar 25 puntos; en caso contrario marque 0.
- Si la pregunta relacionada con efectividad se está cumpliendo, se deben asignar 50 puntos; en caso contrario marque 0.

La evaluación se debe aplicar a cada control definido para el riesgo, determinando si se cumple o no el factor, según corresponda.

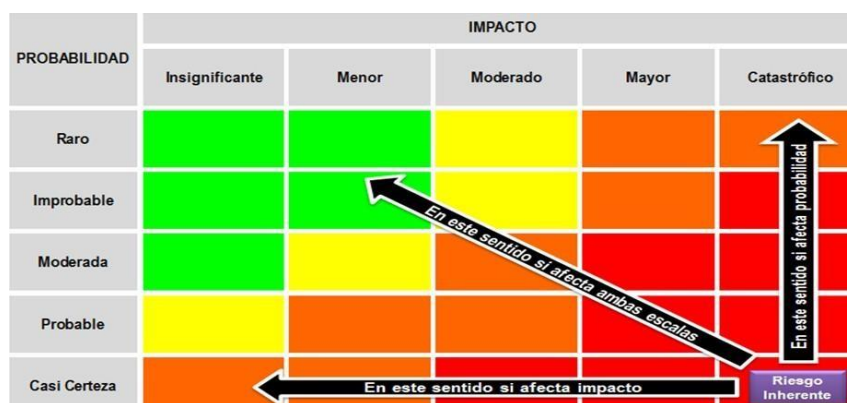
RIESGO RESIDUAL Y DEFINICIÓN DE OPCIONES DE MANEJO

Previo a la definición del riesgo residual se debe determinar qué escala (probabilidad, impacto o ambas) se afecta positivamente con la aplicación del control teniendo en cuenta las siguientes indicaciones:

| Escala de afectación | | |
|--|---|--|
| PROBABILIDAD | IMPACTO | AMBAS |
| Cuando el control está orientado a eliminar o mitigar las causas del riesgos | Cuando el control está orientado a eliminar o mitigar las consecuencias | Cuando el control elimina o mitiga causas y consecuencias del riesgo |

Afectación de escalas según la probabilidad y/o el impacto

La evaluación de los controles (documentación, aplicación y efectividad) definirá la ubicación del riesgo en la matriz de evaluación; este paso se denomina “evaluación del riesgo residual”; los riesgos se pueden desplazar de la siguiente manera según la calificación de los controles y la definición de la escala que afecta cada riesgo.



Afectación de escalas según la probabilidad y/o el impacto

Cuando se ha determinado el riesgo residual se debe asociar la opción de manejo mediante la cual se dará tratamiento al riesgo residual. Las opciones de manejo se determinan teniendo en cuenta la ubicación del riesgo según las zonas definidas así:

| Color | Zona de riesgo | Opciones de manejo |
|-------|-------------------------|---|
| B | Zona de riesgo baja | Asumir el riesgo |
| M | Zona de riesgo moderada | Asumir el riesgo Reducir el riesgo |
| A | Zona de riesgo alta | Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo |
| E | Zona de riesgo extrema | Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo |

- **Asumir el riesgo:** aceptar la pérdida residual probable y elaborar los planes de contingencia para su manejo.
- **Reducir el riesgo:** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). Ej.: optimización de procesos, definición de nuevos controles, entre otros.
- **Evitar el riesgo:** tomar las medidas encaminadas a prevenir su materialización. Ej.: cambios a la infraestructura, cambios en software.
- **Compartir o transferir el riesgo:** reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o mediante otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Ej.: seguros, sitios alternos, contratos de riesgos compartidos, etc.

NOTA:

Este plan será ajustado de acuerdo a los objetivos y metas del plan estratégico 2022- 2025, que se encuentra en construcción.