

INSTITUTO FEDERAL DE TELECOMUNICACIONES



METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS
DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES

UNIDAD DE ADMINISTRACIÓN
DIRECCIÓN GENERAL DE FINANZAS, PRESUPUESTO Y CONTABILIDAD
Dirección de Control Interno y Administración de Riesgos

CONTENIDO

1. INTRODUCCIÓN	1
2. DISPOSICIONES GENERALES.....	2
2.1. SIGLAS	2
2.2. GLOSARIO DE TÉRMINOS	2
3. FUNDAMENTO JURÍDICO.....	4
3.1. ÁMBITO DE APLICACIÓN	5
4. OBJETIVO.....	5
4.1. CONSIDERACIONES PARA LA ADMINISTRACIÓN DE RIESGOS.....	5
4.2. BENEFICIOS DE LA ADMINISTRACIÓN DE RIESGOS	6
5. PROCESO DE LA ADMINISTRACIÓN DE RIESGOS.....	6
6. ETAPAS DEL PROCESO DE LA ADMINISTRACIÓN DE RIESGOS.....	7
6.1 ESTABLECIMIENTO DE OBJETIVOS.....	7
6.2 DEFINICIÓN DE OBJETIVOS DE PROYECTOS, PROCESOS Y/O PROCEDIMIENTOS.....	9
6.3 IDENTIFICACIÓN DE RIESGOS.....	11
6.3.1 REDACCIÓN DEL RIESGO.....	11
6.3.2 DESCRIPCIÓN DEL RIESGO	13
6.3.3 CLASIFICACIÓN DEL RIESGO.....	14
6.4 IDENTIFICACIÓN DE FACTORES DE RIESGO	18
6.5 IDENTIFICACIÓN DE LOS POSIBLES IMPACTOS (CONSECUENCIAS) DE LOS RIESGOS	19
6.6 ANÁLISIS Y EVALUACIÓN DE RIESGOS	20
7. IMPLEMENTACIÓN DE CONTROLES.....	23
7.1 TIPOS DE CONTROLES.....	23
7.2 CARACTERÍSTICAS DE LOS CONTROLES.....	24
7.3 EVALUACIÓN DE CONTROLES.....	25
8. VALORACIÓN FINAL DE RIESGOS RESPECTO A CONTROLES.....	27
8.1 PRIORIZACIÓN FINAL DE RIESGOS	29
9. TOLERANCIA AL RIESGO	29
10. ESTABLECIMIENTO DE LA RESPUESTA AL RIESGO.....	30
10.1 POLÍTICA DE RESPUESTA ANTE LA MATERIALIZACIÓN DEL RIESGO.....	30
11. HERRAMIENTAS PARA LA ADMINISTRACIÓN DE RIESGOS.....	32
11.1 MATRIZ DE ADMINISTRACIÓN DE RIESGOS.....	32
11.2 MAPA INSTITUCIONAL DE RIESGOS.....	33
11.3 EL PROGRAMA ANUAL DE ADMINISTRACIÓN DE RIESGOS (PAAR)	34
11.4 FORMALIZACIÓN DE LA MATRIZ DE ADMINISTRACIÓN DE RIESGOS Y EL MAPA INSTITUCIONAL DE RIESGOS	35
12. INFORMACIÓN Y COMUNICACIÓN.....	35
13. SUPERVISIÓN.....	36

1. INTRODUCCIÓN

La Administración de Riesgos se define como un proceso dinámico para identificar y evaluar los riesgos asociados a los objetivos, el cual se contextualiza como parte del Control Interno conforme al modelo o marco de mayor reconocimiento y aplicación a nivel internacional: COSO1 (por sus siglas en inglés Committee of Sponsoring Organizations of the Treadway Commission), emitido en 1992 y su última actualización en septiembre de 2017, en el cual se establece el concepto de Control Interno y se definen sus componentes.

En la actualidad, el Control Interno tiene una relevancia hacia el interior de las entidades públicas o privadas, al ayudar a lograr el cumplimiento de sus objetivos y metas institucionales con eficiencia, eficacia y economía, fomentando la Integridad y el combate a la corrupción, previniendo la materialización de riesgos que puedan afectar el logro de metas y objetivos, coadyuvando en la obtención y presentación de información financiera y de operación en términos de confiabilidad y oportunidad, favoreciendo el cumplimiento del marco legal y normativo; así como, la transparencia y la rendición de cuentas a los distintos órganos fiscalizadores.

Es importante mencionar que, desde su creación y tomando como base el modelo de Control Interno COSO, el IFT ha llevado a cabo diversas acciones para fortalecer y mejorar el Sistema de Control Interno institucional (SCII); las cuales, incluyen (entre otras) la identificación y la administración de riesgos.

Bajo esa tesitura, se emite la presente Metodología de Administración de Riesgos del Instituto Federal de Telecomunicaciones (en lo sucesivo “Metodología”); mediante la cual, las personas servidoras públicas Responsables de los Proyectos, Procesos y/o Procedimientos del Instituto, empleando una serie de etapas secuenciales podrán identificar y evaluar sus riesgos potenciales, con el fin de minimizar los Factores de riesgos que pudieran afectar el cumplimiento de los objetivos y metas establecidos a nivel estratégico, directivo y operativo proporcionando una Seguridad Razonable respecto su cumplimiento.

¹ Normas de Control Interno del Instituto Federal de Telecomunicaciones. (CONSIDERANDO) Pág. 2. COSO (Comité de Organizaciones Patrocinadoras de la Comisión Treadway), en los Estados Unidos de América; el modelo internacional de control integral COSO está diseñado para apoyar a la dirección en un mejor control de la organización; provee un estándar como fundamento para evaluar el Control Interno e identificar las mejores prácticas aplicables, incluyendo la identificación de los riesgos internos y externos asociados con el cambio, privilegiando la planeación como un elemento indispensable para un control eficaz y evitar prácticas fraudulentas en la información financiera .

2. DISPOSICIONES GENERALES

2.1. SIGLAS

IFT o Instituto: Instituto Federal de Telecomunicaciones o Instituto.

DCIAR: Dirección de Control Interno y Administración de Riesgos.

DGFPC: Dirección General de Finanzas, Presupuesto y Contabilidad.

GTMCIAAR: Grupo de Trabajo en Materia de Control Interno y Administración de Riesgos.

OIC: Órgano Interno de Control del IFT.

PAT: Programa Anual de Trabajo del IFT.

PSP: Persona Servidora Pública del IFT.

SCII: Sistema de Control Interno Institucional.

UA: Unidades Administrativas.

UADM: Unidad de Administración.

2.2. GLOSARIO DE TÉRMINOS

Para efectos de la presente Metodología, se entenderá por:

- I. **Acto contrario a la integridad:** Acción u omisión mediante la cual una persona servidora pública, en ejercicio de las facultades que su cargo le confiere, incurre en uso indebido de recursos o información, con el objeto de beneficiarse a sí mismo o a terceros, causando daño al Instituto.
- I. **Administración de Riesgos:** Es el proceso mediante el cual se identifica, valora y prioriza las actividades que pueden impactar en el cumplimiento de un objetivo, seguido de la coordinación de acciones de control, tratando de mitigar el impacto negativo.
- II. **Componentes del Control Interno:** Los que conforman el Modelo de Control Interno del Instituto: Ambiente de Control; Administración de Riesgos; Actividades de Control; Información y Comunicación, y Supervisión.
- III. **Control Interno.** Es un proceso efectuado por el Comisionado Presidente, los Titulares de Unidad, los Coordinadores Generales, así como por los Directores Generales y Directores Generales Adjuntos con el apoyo de la UADM, y las demás personas servidoras públicas, con objeto de proporcionar una seguridad razonable sobre la consecución de los objetivos institucionales y la salvaguarda de los recursos públicos, así como para prevenir actos contrarios a la integridad.
- II. **Elementos de Control:** Elementos de interés que integran los principios de control, los cuales expresan a nivel de detalle las características que permiten asegurar la implementación, operación y actualización del Control Interno;

- IV. **Estructura organizacional:** Las Unidades Administrativas, procesos sustantivos, estratégicos y adjetivos y cualquier otra estructura utilizada por los Titulares de Unidad, los Coordinadores Generales, así como por los Directores Generales y Directores Generales Adjuntos para lograr los objetivos institucionales.
- V. **Evaluación del riesgo:** Se determina mediante la estimación de la Probabilidad y el Impacto del riesgo. Para realizarla se puede utilizar la información disponible, también pueden emplearse modelos de simulación o hasta técnicas colaborativas.
- VI. **Factor de riesgo:** Es la circunstancia o situación interna y/o externa que aumenta la probabilidad de que un riesgo se materialice.
- VII. **Identificación de riesgos:** Etapa que consiste en identificar el evento adverso que podría afectar el cumplimiento de las metas y objetivos a nivel estratégico, directivo y operativo.
- VIII. **Impacto:** Son las consecuencias negativas que se generarían en el Instituto, en el supuesto de materializarse el riesgo.
- IX. **Integridad:** Principio rector establecido en el Código de Conducta del Instituto que refiere que las personas servidoras públicas actúan siempre de manera congruente con los principios que se deben observar en el desempeño de un empleo, cargo, comisión o función, convencidas en el compromiso de ajustar su conducta para que impere en su desempeño una ética que responda al interés público y generen certeza plena de su conducta frente a todas las personas con las que se vinculen u observen su actuar.
- X. **Matriz de Administración de Riesgos:** El tablero de control y gestión diseñado para identificar, analizar, evaluar y tratar los riesgos asociados a los objetivos estratégicos, operacionales o de información.
- XI. **Mapa Institucional de Riesgos:** Es la representación gráfica de uno o más riesgos que permite vincular la Probabilidad de ocurrencia y su Impacto en forma clara y objetiva.
- XII. **Materialización del Riesgo:** Es la ocurrencia de un evento adverso que amenaza el logro de metas y objetivos del Instituto o la continuidad de las operaciones.
- XIII. **Normas:** Las Normas de Control Interno del Instituto Federal de Telecomunicaciones; que establecen los Principios de Control, así como el diseño, la implementación, los ámbitos de competencia y los mecanismos de evaluación del Control Interno del Instituto.
- XIV. **Principios de control:** Puntos que conforman cada componente del Control Interno, y que se integran de Elementos de Control que, en su conjunto, permiten la implementación, operación y actualización del Control Interno.
- XV. **Probabilidad:** Es la medida (expresada como porcentaje o razón) para estimar la posibilidad de que ocurra un incidente o evento.
- XVI. **Procedimiento:** Nivel menor en la estructura de la gestión de Procesos, que detalla un grupo de actividades y el flujo de éstas para obtener las salidas esperadas, por medio del tratamiento y procesamiento de sus entradas.

- XVII. **Proceso:** Conjunto de Procedimientos y actividades que de manera coordinada y controlada transforman una entrada en una salida conforme a requisitos y reglas específicas.
- XVIII. **Proceso Sustantivo:** Son aquellos que tienen una relación directa con la misión, los objetivos y las estrategias Institucionales. Su ejecución y cumplimiento tendrá un Impacto directo en los sectores de telecomunicaciones y radiodifusión.
- XIX. **Proceso Adjetivo:** Son aquellos dedicados a soportar y asegurar la correcta ejecución de los procesos sustantivos y los procesos estratégicos. Un resultado negativo en su cumplimiento tendrá un Impacto indirecto en los sectores de telecomunicaciones y radiodifusión.
- XX. **Proceso Estratégico:** Aquellos enfocados a la planeación, coordinación y cohesión de las Unidades Administrativas y sus procesos. Su principal finalidad es monitorear y evaluar el funcionamiento del Instituto, así como dictar las pautas que deberán seguir una o varias Unidades Administrativas.
- XXI. **Proyecto:** Es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único, implica una planificación que consiste en un conjunto de actividades que se encuentran interrelacionadas y coordinadas. El propósito de un Proyecto es alcanzar objetivos específicos dentro de los límites que imponen un presupuesto, calidades establecidas previamente y un lapso previamente definido.
- XXII. **Responsables de los Procesos:** Personas Servidoras Públicas adscritas a las Unidades Administrativas que, de conformidad con su grado jerárquico, son encargados de dirigir, ejecutar, controlar y administrar las actividades de los procesos operativos.
- XXIII. **Respuesta al riesgo:** Son las actividades determinadas y específicas que elige el Instituto para evitar o prevenir, reducir, dispersar, transferir y asumir riesgos.
- XXIV. **Riesgo (Inherente):** Posibilidad de que ocurra un evento que afecte negativamente el logro de las metas y objetivos del Instituto; en ausencia de acciones de control para disminuir su Probabilidad o Impacto.
- XXV. **Riesgo residual:** Es el nivel de Riesgo que permanece posterior a la implementación de controles para mitigar la Probabilidad e Impacto del Riesgo inherente;
- XXVI. **Seguridad Razonable:** Alto nivel de confianza, mas no absoluto, de que los objetivos del Instituto serán alcanzados.
- XXVII. **Sistema de Control Interno Institucional o SCII:** Conjunto de normas, proyectos, procesos, políticas y procedimientos, que establecen principios, objetivos, metodologías y evaluaciones para el cumplimiento de los objetivos Institucionales
- XXVIII. **Tolerancia al Riesgo:** Es el nivel aceptable de variación en los resultados o actuaciones de la institución relacionada con la consecución o logro de los objetivos. Es la cantidad máxima de un Riesgo que las Unidades Administrativas del Instituto puedan soportar sin causar graves daños al logro de los objetivos institucionales.

3. FUNDAMENTO JURÍDICO

- Artículo 60, fracción XIII, del Estatuto Orgánico del Instituto Federal de Telecomunicaciones

- Artículo 6, fracción II, de las Normas de Control Interno del IFT.

3.1. ÁMBITO DE APLICACIÓN

En concordancia con el artículo 2 de las Normas, la presente Metodología es de observancia general y obligatoria para todas las personas servidoras públicas de las UA del Instituto, con excepción de la Autoridad Investigadora y el Órgano Interno de Control (OIC), quienes están dotados de autonomía técnica y de gestión para decidir sobre su funcionamiento y resoluciones, y las cuales podrán adoptarlas en el caso de que así lo determinen.

Asimismo, de conformidad con lo dispuesto en el artículo 7, fracciones IV y V, de las Normas; es competencia del Comisionado Presidente; aprobar la presente Metodología; así como, aprobar los mecanismos para la promoción de la cultura de Control Interno, Integridad, y administración de riesgos que proporciona un respaldo y patrocinio como máxima autoridad del SCII.

4. OBJETIVO

Establecer un proceso sistemático y dinámico realizado por las UA, de conformidad con las competencias establecidas en las Normas, que permita desarrollar el componente de Administración de Riesgos por medio del análisis, identificación, evaluación, respuesta, supervisión, comunicación y seguimiento a los Riesgos, incluidos los relacionados con actos contrarios a la Integridad, inherentes o asociados a los proyectos, procesos y/o procedimientos del Instituto mediante el análisis de los distintos factores que pueden provocarlos.

Lo anterior, con la finalidad de definir las estrategias y acciones que permitan mitigarlos y asegurar, de una forma razonable, el cumplimiento de los objetivos institucionales en términos de eficacia, eficiencia y economía en un marco de transparencia y rendición de cuentas, de conformidad con el nivel de tolerancia al riesgo que hayan establecido las UA.

4.1. CONSIDERACIONES PARA LA ADMINISTRACIÓN DE RIESGOS.

1. El Riesgo es inherente a todos los proyectos, procesos y/o procedimientos que lleva a cabo el Instituto en el cumplimiento de sus atribuciones.
2. La presente Metodología se enfoca en la Identificación de Riesgos inherentes, tanto a los objetivos de las UA, como a los proyectos, procesos y/o procedimientos, por lo que esta metodología se considera una herramienta de aplicación general.
3. El diseño de controles a nivel operacional es responsabilidad de las PSP Responsables de las UA y de los proyectos, procesos y/o procedimientos.
4. No existe ninguna forma de reducir el Riesgo a cero.
5. Los Riesgos son administrados, tomando en consideración el contexto en el que se desenvuelve el Instituto y el establecimiento de controles a cada factor de riesgo identificado.

4.2. BENEFICIOS DE LA ADMINISTRACIÓN DE RIESGOS ²

1. Agrega valor a los procesos.
2. Es útil para la toma de decisiones.
3. Es sistemática y estructurada.
4. Toma en cuenta los diferentes tipos de factores que puedan impactar en el cumplimiento de objetivos.
5. Contribuye a la transparencia y rendición de cuentas.
6. Promueve la mejora continua.

5. PROCESO DE LA ADMINISTRACIÓN DE RIESGOS

De acuerdo con las Normas, la Administración de Riesgos en el Instituto se enfoca en identificar y mitigar los Riesgos asociados o inherentes a los objetivos de los proyectos, procesos y/o procedimientos, incluidos los relacionados con actos contrarios a la Integridad mediante el análisis de sus características y funcionamiento, por lo que se considera como una herramienta de aplicación general.

Lo anterior se realiza mediante un proceso, el cual es coordinado por la DGFP; en el que se establecen los procedimientos y formas para identificar, evaluar, analizar, responder, controlar, supervisar y comunicar los Riesgos institucionales de forma anual.

El proceso de Administración de Riesgos se podrá apoyar de cualquier herramienta tecnológica o sistema automatizado para gestionar los Riesgos institucionales, con la finalidad de que la Administración de Riesgos pueda concebirse y llevarse a cabo de una forma práctica y lógica al interior de las UA y considerando los principales elementos de supervisión y comunicación que dicho proceso requiere.

Finalmente, la Administración de Riesgos se implementa a través de la programación de actividades, cuyo objetivo es definir las etapas del proceso de administración de riesgos y, en su caso, la participación de los distintos actores que en él intervienen, las cuales se podrán definir de modo general (no concluyente ni limitativa) de la manera siguiente:

1. Inicio del proceso, mediante la celebración de reunión coordinada por la DGFP con el GTMCIAR.
2. La DGFP realizará acciones de capacitación para el GTMCIAR, destinadas al desarrollo del proceso.
3. Actualización de la Matriz de Administración de Riesgos de cada UA, por parte de los Responsables de los proyectos, procesos y/o procedimientos, con el apoyo y coordinación de los respectivos enlaces del GTMCIAR.
4. Revisión de la Matriz de Administración de Riesgos conforme a la actualización realizada por cada UA, verificando que cumpla con lo establecido en la Metodología de Administración de Riesgos.
5. Elaboración de la Matriz de Administración de Riesgos por UA e institucional por parte de la DCIAR; así como, los mapas de Riesgos correspondientes.
6. Implementar actividades de coordinación entre la DCIAR y el GTMCIAR, para formalizar las matrices de Riesgos por cada UA, con el apoyo de los Titulares de Unidad, Coordinadores Generales y la DGFP.

² Fuente: Auditoría Interna: Servicios de aseguramiento y consultoría – La fundación de investigaciones del Instituto de Auditores Internos, 2009

7. Elaboración del Informe Anual del Estado que Guarda el SCII, el cual incluye la Matriz de Administración de Riesgos y el Mapa Institucional de Riesgos.
8. Elaboración del Programa Anual de Administración de Riesgo, el cual es autorizado por el Comisionado Presidente.

Las actividades anteriormente enlistadas, podrán ser realizadas durante el ejercicio corriente, debiendo culminar en el último trimestre de cada año; con el fin de contar con la información suficiente, pertinente y oportuna para el Informe Anual del Estado que Guarda el Sistema de Control Interno Institucional.

6. ETAPAS DEL PROCESO DE LA ADMINISTRACIÓN DE RIESGOS

Identificar y evaluar los Riesgos le permite a las PSP del Instituto estar conscientes de los eventos adversos que pueden enfrentar en el cumplimiento de objetivos, así como de las estrategias que deben implementar para prevenirlos o controlarlos; en consecuencia, es su función y responsabilidad en el proceso de la Administración de Riesgos.

6.1 ESTABLECIMIENTO DE OBJETIVOS.

El Instituto deberá establecer un plan estratégico que oriente sus esfuerzos hacia la consecución de los objetivos institucionales, la misión, visión y se asocie al mandato legal, que permita la alineación de los objetivos de los proyectos, procesos y/o procedimientos.

El primer paso para la identificación, análisis, evaluación y determinación del Riesgo y de una respuesta, es conocer los posibles eventos en el entorno interno y externo que podrían influir en el logro de los objetivos de los proyectos, procesos y/o procedimientos que llevan a cabo las UA, los cuales contribuyen al cumplimiento de los objetivos institucionales.

Una vez concluido este análisis del contexto, las PSP Responsables de los proyectos, procesos y/o procedimientos estarán en posibilidad de iniciar el proceso de Administración de Riesgos; a continuación, se muestran las principales etapas para administrar de forma correcta los Riesgos a los que se enfrentan las UA.

Evaluar el entorno de los proyectos, procesos y/o procedimientos tanto interno como externo, lo cual permite estar consciente de las circunstancias o situaciones que rodean a éstos, y a su vez, identificar los riesgos y las estrategias para prevenirlos o controlarlos. Este proceso se realizará conforme a lo siguiente:

- Identificar el entorno interno del Instituto, pudiendo basarse en ejercicios anteriores de identificación y administración de riesgos, auditorías, revisiones de control y/o revisiones internas y autoevaluaciones, en cuanto a aspectos de estructura organizacional general y particular de las UA, la normatividad interna, el cumplimiento de ésta, valores institucionales, capital humano, recursos materiales, financieros y tecnológicos, seguridad interna, eventos adversos presentados; lo anterior de manera enunciativa, de tal manera que permita conocer el ambiente y contexto institucional que prevalece en ese momento al interior del Instituto.
- Identificar el entorno externo del Instituto a nivel local, nacional e internacional, en lo relativo a legislaciones, ambiente político, intereses de gobiernos, instituciones y empresas homólogas; así como las regulaciones que puedan afectar el quehacer del Instituto, los tratados y convenciones internacionales, el ambiente sociocultural; los aspectos de seguridad externa, la política monetaria, los eventos naturales y los avances tecnológicos, etc.

- Identificar, seleccionar y agrupar diversas situaciones que puedan afectar los proyectos, procesos y/o procedimientos del Instituto, considerando lo siguiente:
 - a) La estructura del Instituto y la estructura material y de los sistemas.
 - b) Los procesos establecidos en las unidades administrativas.
 - c) Los objetivos de los proyectos, procesos y/o procedimientos.
 - d) Las atribuciones estatutarias de cada unidad administrativa.
 - e) Las estrategias establecidas en el Programa Anual de Trabajo y en la Hoja de Ruta vigente.
 - f) Los recursos presupuestarios asignados al Instituto y los recursos autogenerados.
 - g) El desempeño institucional y el ejercicio de los recursos.
- Analizar el comportamiento histórico de los riesgos identificados en ejercicios anteriores considerando los elementos siguientes:
 - a) Eventos materializados en el último año calendario.
 - b) Estadística registrada por las PSP responsables de los proyectos, procesos y/o procedimientos sobre riesgos materializados en años anteriores.
 - c) Comparativos anuales que realicen las UA sobre el comportamiento de los riesgos, que permita conocer la reincidencia de éstos, su impacto y, de ser el caso, nuevos factores de riesgo que hayan surgido, así como acciones implementadas para la administración de esos riesgos.

Una vez concluido este análisis del entorno interno y externo, así como del comportamiento histórico de los riesgos institucionales, los responsables de los procesos están en posibilidad de iniciar el proceso de Administración de Riesgos.

TABLA 1. ETAPAS DEL PROCESO DE ADMINISTRACIÓN DE RIESGOS

INFORMACIÓN Y COMUNICACIÓN	Establecimiento de objetivos y metas	Es la definición de los objetivos a nivel institucional que permite la identificación y evaluación de los Riesgos potenciales asociados a éstos. Las UA deben establecer un objetivo por cada proyecto, proceso y/o procedimiento, el cual debe de estar alineado con la planeación estratégica y considerar los entornos externo e interno que permitan el diseño y la implementación del Control Interno.	SUPERVISIÓN
	Identificación de Riesgo	Se identifica el evento adverso a la consecución del objetivo o meta establecido para cada proyecto, proceso y/o procedimiento.	
	Identificación de Factores de Riesgo	Mediante el análisis del contexto interno y externo, actual y pasado en el que se desarrollan los proyectos, procesos y/o procedimientos; con la finalidad de, identificar los diversos factores (causa) que pueden propiciar la materialización (efecto) del Riesgo; empleando diversas técnicas especializadas para ello.	

Análisis, valoración inicial y priorización de Riesgos	<p>Una vez, identificados los Factores de Riesgo, se debe determinar la Probabilidad e Impacto de que el Riesgo se materialice (nivel de criticidad) sin la implementación de controles, con la finalidad de visualizar la criticidad del Riesgo y priorizarlo considerando, lo siguiente:</p> <ul style="list-style-type: none"> • El posible Impacto y Probabilidad de ocurrencia que representa la materialización de los Riesgos identificados en perjuicio del logro de los objetivos institucionales. • Los Riesgos en términos de mayor a menor Impacto y frecuencia para definir las acciones a corto y mediano plazo para su mitigación.
Implementación de controles	Establecer mecanismos de control para mitigar los efectos contrarios al logro de objetivos provocados por la posible materialización de los Factores de Riesgo dentro de los proyectos, procesos y/o procedimientos y evaluar su efectividad.
Valoración final de Riesgos respecto a controles.	Se define la valoración del Riesgo residual, como el resultado de la implementación y efectividad de los controles establecidos para mitigarlos Factores de Riesgos, respecto de la valoración inicial realizada de los Factores de Riesgos en los Procesos, Programas y Proyectos institucionales.
Establecimiento de la Respuesta al Riesgo.	<p>Se establecen las estrategias por cada UA para administrar los Riesgos en sus proyectos, procesos y/o procedimientos considerando:</p> <ul style="list-style-type: none"> • El plan de acción para mitigar, principalmente, los Riesgos evaluados con alto Impacto y Probabilidad de ocurrencia. • Un periodo en el que se definan fechas de implementación del plan y sus responsables.

6.2 DEFINICIÓN DE OBJETIVOS DE PROYECTOS, PROCESOS Y/O PROCEDIMIENTOS.

Las UA deben definir objetivos en términos específicos, medibles y alcanzables, los cuales deberán alinearse con los objetivos establecidos en el plan estratégico, la misión y visión Institucionales que permitan mitigar los riesgos por medio del establecimiento de mecanismos de control, considerando lo siguiente:

- La estructura orgánica del Instituto y de cada UA.
- Las atribuciones en el ámbito de su competencia, de acuerdo con el Estatuto Orgánico, el Manual de Organización General y los Manuales de Organización Específicos y de Procedimientos.
- Los programas de trabajo destinados al cumplimiento de los objetivos de cada UA.
- La documentación de los proyectos, procesos y/o procedimientos.

El establecimiento de objetivos de los proyectos, procesos y/o procedimientos es de gran importancia para la Administración de Riesgos, debido a que a partir de éstos se logran identificar los eventos adversos que podrían impactar en su cumplimiento; para su definición se pueden considerar los aspectos que se señalan a continuación.

1. Para redactar el objetivo se debe de responder a la pregunta ¿para qué se realiza? y es conveniente complementarla con la respuesta a la pregunta ¿mediante qué instrumentos se realiza?

2. La estructura del objetivo es una acción principal expresada con un verbo en infinitivo más los medios utilizados
3. El objetivo es el propósito que se pretende alcanzar mediante la ejecución de las etapas del Proceso.
4. Se recomienda que el objetivo se encuentre documentado.

Objetivos a nivel operativo:

- a) Los objetivos del proceso están orientados a definir determinados resultados precisos, cuantificables y en plazos específicos. Estos objetivos determinan lo que debe lograr el proceso en términos de productividad, calidad, costo, precisión, cumplimiento y satisfacción de la ciudadanía.
- b) Los objetivos de un procedimiento son los resultados que se pretenden alcanzar en lo individual para cumplir con el objetivo del proceso principal; por lo que no debe ser un listado de actividades a realizar.
- c) Los objetivos de un proyecto son los resultados específicos y medibles que se pretende lograr en un plazo definido de acuerdo con el cronograma de cada proyecto particular. Dejan claro cuál es el propósito de éste y guían al equipo hasta completarlo de forma satisfactoria.

Ejemplos:

Objetivo establecido a nivel Proceso

PROCESO	OBJETIVO DIRECTIVO
Control Interno y Administración de Riesgos	Coordinar, evaluar y dar seguimiento al Sistema de Control Interno Institucional, para dar una Seguridad Razonable sobre la consecución de los objetivos institucionales y la salvaguarda de los recursos públicos, así como para prevenir actos contrarios a la Integridad.

Objetivo establecido a nivel Procedimiento

PROCESO	PROCEDIMIENTO	OBJETIVO OPERATIVO
Control Interno y Administración de Riesgos	Control Interno Institucional	Coordinar, evaluar y dar seguimiento a la implementación del Control Interno conforme a lo establecido en las Normas de Control Interno.

En la Matriz de Administración de Riesgos; el objetivo de las UA se establece en el campo "Objetivo" como se puede ver a continuación:

(el ejemplo corresponde al objetivo del Proceso):

OBJETIVO	PROYECTO, PROCESO Y/O PROCEDIMIENTO
Coordinar, evaluar y dar seguimiento al Sistema de Control Interno Institucional, para dar una Seguridad Razonable sobre la consecución de los objetivos institucionales y la salvaguarda de los recursos públicos, así como para prevenir actos contrarios a la Integridad.	(Estratégico) Control Interno y Administración de Riesgos

6.3 IDENTIFICACIÓN DE RIESGOS

La Identificación de Riesgos es una actividad que se debe realizar de forma continua y periódica en las funciones sustantivas, estratégicas y adjetivas del Instituto. Dicha actividad es realizada por las PSP Responsables de éstas.

Para llevar a cabo la Identificación de Riesgos se pueden emplear diversas técnicas y herramientas que se mencionan a continuación

TABLA 2. TÉCNICAS Y/O HERRAMIENTAS DE IDENTIFICACIÓN DE RIESGOS

TÉCNICA Y/O HERRAMIENTA DE IDENTIFICACIÓN	DESCRIPCIÓN
Talleres de Autoevaluación	Realizar reuniones con personas servidoras públicas de diferentes niveles jerárquicos que desempeñen actividades clave en el Instituto, con el propósito de identificar los Riesgos, analizar y evaluar su posible Impacto en el cumplimiento de los objetivos y proponer acciones para su mitigación.
Mapeo de Procesos	Revisar el diagrama del procedimiento e identificar los puntos críticos que podrían implicar un Factor de Riesgo. Para efectuarla es necesario que se encuentre documentado el Proceso.
Analizar los escenarios del entorno interno y externo (supuestos de materialización de Riesgos)	Revisión de cambios en el marco legal, entorno económico o cualquier factor interno o externo que podría amenazar el cumplimiento de los objetivos.
Análisis comparativo de Indicadores de gestión, desempeño y Riesgos	Análisis para evaluar sus desviaciones, es decir, que su comportamiento se encuentra por encima o debajo del rango normal, esto debe analizarse para determinar si esa desviación se debe por algún Riesgo materializado o su comportamiento anormal tiene alguna explicación diferente a un Riesgo.
Entrevistas con los responsables y ejecutantes de los Procesos,	Aplicación de una serie de preguntas relacionadas con los eventos que amenazan el logro de los objetivos. Se aplican a PSP de diferentes niveles jerárquicos de una o varias unidades administrativas.
Cuestionarios de Identificación de Riesgos y controles, dirigidos a PSP de todos los niveles jerárquicos.	Aplicación de una serie de preguntas enfocadas a detectar las preocupaciones de las PSP de mandos superiores, medios u operativos sobre Riesgos que se perciben en las actividades que desempeñan.

6.3.1 REDACCIÓN DEL RIESGO

El nombre que se asigne al Riesgo debe indicar con precisión cuál es el evento contrario o adverso que impide el logro del objetivo del proyecto, proceso y/o procedimiento, por lo que se recomienda no caer en textos con demasiada extensión literaria o ambigüedades que propicien perder de vista cuál es la afectación directa por la Materialización del Riesgo.

El nombre del Riesgo deberá estructurarse con los elementos siguientes:

Sustantivo + Verbo en participio + Adjetivo, Adverbio o Complemento o circunstancia negativa

Figura 1



Esquema elaborado por el IFT

Recomendaciones:

- Redactar el Riesgo de forma clara, específica y directa, sin dar lugar a ambigüedades.
- Utilice pocas palabras para redactar el nombre del Riesgo.
- Procurar evitar calificativos como “malo” o “poco”; prefiera otros más precisos como “deficiente”, “insuficiente” o “ineficiente”.

Ejemplos de Riesgos redactados correctamente:

- Trámites realizados sin los estándares de calidad.
- Trámites otorgados fuera del plazo establecido.
- Proveedores y personas servidoras públicas coludidos en la asignación de contratos.
- Expedientes elaborados sin considerar lo establecido en la normativa.
- Informes anuales elaborados deficientemente.

Ejemplos incorrectos de la redacción de un Riesgo:

- Mala actuación de los servidores públicos.
- No cumplir con los objetivos de los Programas.
- Inadecuada aplicación de la normatividad por desconocimiento o interpretación indebida.
- Presentación extemporánea u omisión de la declaración patrimonial.

Asimismo, se ponen a su consideración las sugerencias siguientes para su redacción:

1. Identificar el objetivo operativo del proyecto, proceso y/o procedimiento.
2. Buscar en el objetivo lo siguiente:
 - a) El sustantivo del objetivo.
 - b) Identificar la actividad realizada (descrita como el verbo o acción principal).
 - c) Reconocer la situación o situaciones positiva(s) que persigue el objetivo para trasladarla a una situación (es) en negativo que sirva de base para identificar el complemento negativo.
3. El nombre del Riesgo debe guardar concordancia con el objetivo del proyecto, proceso y/o procedimiento.

Ejemplo 1: Redacción del nombre del Riesgo a nivel Proceso

PROCESO	OBJETIVO DIRECTIVO
Control Interno y Administración de Riesgos	Coordinar, evaluar y dar seguimiento al Sistema de Control Interno institucional, para dar una Seguridad Razonable sobre la consecución de los objetivos institucionales y la salvaguarda de los recursos públicos.

Sustantivo descrito en el objetivo:	Sistema de Control Interno Institucional
Acción principal en forma de verbo	Coordinar, evaluar, seguir
Situación positiva que persigue el objetivo	Brindar una seguridad razonable sobre la consecución de los objetivos institucionales y la salvaguarda de los recursos públicos

Ahora, identificamos el Riesgo como uno de los posibles eventos adversos a la consecución del objetivo, de conformidad con la estructura sugerida:

SUSTANTIVO	VERBO EN PARTICIPIO	COMPLEMENTO NEGATIVO
Sistema de Control Interno Institucional	Coordinado, evaluado y con seguimiento	Deficiente

El Riesgo identificado es: *Sistema de Control Interno Institucional coordinado, evaluado y con seguimiento deficiente.*

Ejemplo 2: Identificación del Riesgo a nivel Procedimiento

PROCESO	PROCEDIMIENTO	OBJETIVO OPERATIVO
Control Interno y Administración de Riesgos	Control Interno Institucional	Coordinar, evaluar y dar seguimiento a la implementación del control interno conforme a lo establecido en las Normas de Control Interno.

Sustantivo descrito en el objetivo:	Control
Acción principal en forma de verbo	Coordinar, evaluar y dar seguimiento
Situación positiva que persigue el objetivo	Conforme a lo establecido en las Normas de Control Interno.

SUSTANTIVO	VERBO EN PARTICIPIO	COMPLEMENTO NEGATIVO
Control Interno	Coordinado, evaluado y con seguimiento	En contravención de las Normas de Control Interno

El Riesgo identificado es: *Control Interno coordinado evaluado y con seguimiento contraviniendo las Normas de Control Interno*

En la Matriz de Administración de Riesgos; el nombre del Riesgo se integra en el campo "Nombre del Riesgo" como se puede ver a continuación

NOMBRE DEL RIESGO A NIVEL PROCESO
Sistema de Control Interno Institucional coordinado, evaluado y con seguimiento deficiente.

6.3.2 DESCRIPCIÓN DEL RIESGO

Es una explicación más detallada del significado del Riesgo, donde se explique con mayor precisión la afectación directa al objetivo del Proceso, por lo que se recomienda proporcionar una descripción literal extendida del significado del nombre del Riesgo.

DESCRIPCIÓN DEL RIESGO
<p>Describir brevemente el significado del nombre de Riesgo estructurado</p> <p>"Al no coordinar, evaluar o dar seguimiento de forma correcta el Sistema de Control Interno Institucional no se garantiza la consecución de los objetivos institucionales.</p>

6.3.3 CLASIFICACIÓN DEL RIESGO

El proceso de identificación incluye la clasificación de los Riesgos, para esto se debe considerar por lo menos las siguientes categorías conforme a los Factores de Riesgo que se identifiquen como afectaciones a los proyectos, procesos y/o procedimientos:

Tabla 3. Clasificación de los Riesgos

Clase de Riesgo	Descripción
Estratégico:	Se asocia a los asuntos relacionados con la misión y el cumplimiento de los objetivos estratégicos.
Financiero:	Se relaciona con los recursos económicos de la institución, principalmente de la eficiencia y transparencia en el manejo de los recursos.
Tecnológico:	Se relaciona con la capacidad de la institución para que las herramientas tecnológicas soporten el logro de los objetivos estratégicos.
Operativo:	Este rubro considera los Riesgos relacionados con la inadecuada ejecución de los proyectos, procesos y/o procedimientos.
Legal:	Afecta la capacidad de la institución para dar cumplimiento a la legislación y obligaciones contractuales.
A la reputación o Imagen:	Se refleja en un Impacto de la opinión pública respecto de la labor del Instituto por la materialización de cualquier tipo de Riesgo.
Contrarios a la Integridad	El riesgo de (contra la) integridad, es la ocurrencia de un hecho tal, que el interés público quedaría relegado a un interés privado, generando un potencial impacto negativo para el Instituto.

IDENTIFICACIÓN DE RIESGOS SUSCEPTIBLES DE ACTOS CONTRARIOS A LA INTEGRIDAD

Se debe considerar la posibilidad de ocurrencia de actos contrarios a la integridad relacionados con la inadecuada salvaguarda de los recursos públicos, principalmente de los procesos financieros, presupuestales, de contratación, etc.

Las conductas contrarias a la integridad previstas en la Ley General de Responsabilidades Administrativas y que constituyen faltas graves de las PSP, relacionadas con los riesgos contrarios a la integridad son:

- a) El cohecho; es cuando la PSP que exija acepte, obtenga o pretenda obtener, por sí o a través de terceros, con motivo de sus funciones; cualquier beneficio no comprendido en su remuneración como PSP, que podría consistir en dinero; valores; bienes muebles o inmuebles, incluso mediante enajenación en precio notoriamente inferior al que se tenga en el mercado; donaciones; servicios; empleos y demás beneficios indebidos para sí o para su cónyuge, parientes consanguíneos, parientes civiles o para terceros con los que tenga relaciones profesionales, laborales o de negocios, o para socios o sociedades de las que el servidor público o las personas antes referidas formen parte.
- b) El peculado; es cuando la PSP que autorice, solicite o realice actos para el uso o apropiación para sí o para otras personas, de recursos públicos, sean materiales, humanos o financieros sin fundamento jurídico o en contraposición a las normas aplicables.
- c) El desvío de recursos públicos es cuando la PSP que autorice, solicite o realice actos para la asignación o desvío de recursos públicos, sean materiales, humanos o financieros, sin fundamento jurídico o en contraposición a las normas aplicables.
- d) La utilización indebida de información privilegiada la que obtenga la PSP con motivo de sus funciones y que no sea del dominio público y que adquiera para sí o para otras personas, bienes inmuebles, muebles y valores que pudieren incrementar su valor o, en general, que mejoren sus condiciones, así como obtener cualquier ventaja o beneficio privado, como resultado de información privilegiada de la cual haya tenido conocimiento.
- e) El abuso de funciones, cuando la PSP que ejerza atribuciones que no tenga conferidas o se valga de las que tenga, para realizar o inducir actos u omisiones arbitrarios, para generar un beneficio para sí o otras personas para causar perjuicio a alguna persona o al servicio público; así como cuando realiza por sí o a través de un tercero, alguna de las conductas descritas en el artículo 20 Ter, de la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia.
- f) La actuación bajo conflicto de interés, cuando la PSP que intervenga por motivo de su empleo, cargo o comisión en cualquier forma, en la atención, tramitación o resolución de asuntos en los que tenga conflicto de interés o impedimento legal.
- g) La contratación indebida, cuando la PSP que autorice cualquier tipo de contratación; así como la selección, nombramiento o designación, de quien se encuentre impedido por disposición legal o inhabilitado por resolución de autoridad competente para ocupar un empleo, cargo o comisión en el servicio público o inhabilitado para realizar contrataciones con los entes públicos, siempre que en el caso de las inhabilitaciones, al momento de la autorización, se encuentren inscritas en el sistema nacional de servidores públicos y particulares sancionados de la plataforma digital nacional.
- h) El enriquecimiento oculto u ocultamiento de conflicto de interés, cuando la PSP falte a la veracidad en la presentación de las declaraciones de situación patrimonial o de intereses, que tenga como fin ocultar, respectivamente, el incremento en su patrimonio o el uso y disfrute de bienes o servicios que no sea explicable o justificable, o un Conflicto de Interés.

- i) La simulación de acto jurídico cuando la PSP utilice personalidad jurídica distinta a la suya para obtener, en beneficio propio o de algún familiar hasta el cuarto grado por consanguinidad o afinidad, recursos públicos en forma contraria a la ley.
- j) El tráfico de influencias cuando la PSP utilice la posición que su empleo, cargo o comisión le confiere para inducir a que otra PSP efectúe, retrase u omita realizar algún acto de su competencia para generar cualquier beneficio, provecho o ventaja para sí o para algunas otras personas ajenas a la actividad; o bien cuando la PSP es inducida por un particular que use su influencia, poder económico o político, real o ficticio, con el propósito de obtener para sí o para un tercero un beneficio o ventaja, o para causar perjuicio a alguna persona o al servicio público, con independencia de la aceptación la PSP o del resultado obtenido.
- k) El encubrimiento, cuando la PSP cuando en el ejercicio de sus funciones llegare a advertir actos u omisiones que pudieren constituir faltas administrativas, realice deliberadamente alguna conducta para su ocultamiento.
- l) El desacato, cuando la PSP tratándose de requerimientos o resoluciones de autoridades fiscalizadoras, de control interno, judiciales, electorales o en materia de defensa de los derechos humanos o cualquier otra competente, proporcione información falsa, así como no dé respuesta alguna, retrase deliberadamente y sin justificación la entrega de la información, a pesar de que le hayan sido impuestas medidas de apremio conforme a las disposiciones aplicables.
- m) El nepotismo, cuando la PSP valiéndose de las atribuciones o facultades de su empleo, cargo o comisión, directa o indirectamente, designe, nombre o intervenga para que se contrate como personal de confianza, de estructura, de base o por honorarios en el ente público en que ejerza sus funciones, a personas con las que tenga lazos de parentesco por consanguinidad hasta el cuarto grado, de afinidad hasta el segundo grado, o vínculo de matrimonio o concubinato.
- n) La obstrucción de la justicia cuando las PSP realicen cualquier acto que simule conductas no graves durante la investigación de actos u omisiones calificados como graves en la Ley General de Responsabilidades Administrativas y demás disposiciones aplicables.
- o) El soborno cuando las PSP realicen o se abstengan de realizar un acto relacionado con sus funciones o con las de otra PSP, o bien, abusen de su influencia real o supuesta, con el propósito de obtener o mantener, para sí mismo o para un tercero, un beneficio o ventaja, con independencia de la aceptación o recepción del beneficio o del resultado obtenido ofrecido por un particular.
- p) La colusión, cuando la PSP en contubernio con uno o varios particulares, ejecuten cualquier acción que implique o tenga por objeto o efecto obtener un beneficio o ventaja indebidos en las contrataciones públicas de carácter federal, local o municipal, o la obtención de trámites o resoluciones favorables para conseguir concesiones de bandas del espectro radioeléctrico.

Asimismo, se consideran actos contrarios a la integridad:

- El favoritismo político.
- El robo de bienes.

- La falsificación de datos.
- La filtración de información reservada, confidencial o con datos personales.
- La pérdida o destrucción intencional de documentos oficiales.
- La falta de transparencia.
- La extorsión.

Con el fin de identificar de manera más precisa y oportuna los riesgos contrarios a la integridad, es conveniente considerar aquellos procesos, sin ser limitativos, en los que se ha identificado el mayor número de factores de riesgo y que podrían ser más vulnerables a este tipo de acontecimientos, como los que se señalan a continuación:

Proceso	Concepto
1.- Adquisiciones	Todos aquellos servicios cuya prestación genera una obligación de pago para el Instituto ³ .
2.- Gestión presupuestal y recursos financieros	Se refieren al uso de los recursos patrimoniales y del Fideicomiso disponible para ser empleado en forma de efectivo, valores líquidos y líneas de crédito.
3.- Gestión de talento y pago de remuneraciones	Están relacionados con el reclutamiento, capacitación y pago de salario del personal.
4.- Recursos materiales, servicios generales y contrataciones diversas	Consisten en la administración y distribución de bienes, insumos y servicios, así como en el manejo de almacenes a nivel general ⁴ .
5.- Supervisión, Verificación, Dictaminación	Están relacionados con las actividades sustantivas del Instituto relativas a la supervisión del espectro radioeléctrico.
6.- Atención de trámites con concesionarios y permisionarios y con la ciudadanía	Los procesos sustantivos inherentes a la interacción del Instituto con concesionarios y permisionarios para atender todo lo relacionado con concesiones.
7.- Seguimiento de sanciones	Se refieren al seguimiento que el Instituto debe dar a las sanciones impuestas por incumplimiento de concesionarios y permisionarios.

Ejemplo:

PROCESO	RIESGO IDENTIFICADO
Control Interno y Administración de Riesgos	Sistema de Control Interno Institucional coordinado, evaluado y con seguimiento deficiente.
Clasificación del Riesgo	"OPERATIVO" Clasificación determinada para el ejemplo en virtud de que los factores de riesgo se relacionan con la ejecución del proceso.

En la Matriz de Administración de Riesgos; la clasificación del Riesgo se integra en el campo "Clasificación del Riesgo" como se puede ver a continuación:

CLASIFICACIÓN DEL RIESGO
OPERATIVO

³ En concordancia con el Artículo 3, Ley de adquisiciones, arrendamientos y servicios del sector público.

⁴ Artículo 3, Acuerdo por el que se establecen las disposiciones en Materia de Recursos Materiales y Servicios Generales.

6.4 IDENTIFICACIÓN DE FACTORES DE RIESGO

Los Factores de Riesgo son las causas o situaciones que pueden afectar el cumplimiento de los objetivos institucionales, directivos y operativos que inciden en el aumento de la Probabilidad e Impacto de que un Riesgo se materialice, por lo que las PSP Responsables deberán tomar en consideración los puntos siguientes para su identificación:

- a) Los cambios que se presentan en el entorno, los cuales se dividen en:
 - **Factores Internos:** Eventos o circunstancias generados al interior del Instituto que, pueden llegar a tener una incidencia de Riesgo en los proyectos, procesos y/o procedimientos institucionales.
 - **Factores Externos:** Eventos o circunstancias generados fuera de la esfera de competencia del Instituto y que pueden tener una incidencia de Riesgo en los proyectos, procesos y/o procedimientos institucionales.
- b) Todo proyecto, proceso y/o procedimiento que permite el cumplimiento de un objetivo presenta Factores de Riesgo, por lo que es erróneo señalar que no existen Factores de Riesgo o que es muy remota la posibilidad de su ocurrencia; lo que sucede es que se han implementado los controles necesarios para que no se materialicen, por ello, en algunos casos, se llega a considerar su inexistencia.
- c) El Factor de Riesgo es una circunstancia o situación que aumenta la Probabilidad de que un Riesgo se materialice, por ejemplo, cambios en la Estructura organizacional, modelo operativo, incremento en las actividades realizadas, pandemias, sismos, etc.
- d) Los factores son inherentes a las actividades que realizamos de forma diaria en los Procesos, por lo que siempre existen y están presentes y se deben de controlar de forma adecuada.
- e) Para la identificación de Factores de Riesgo externo se pueden tomar en cuenta elementos creados en el entorno fuera del Instituto pero que afecten las actividades del Proceso mismo, como pueden ser: cambios en la Ley Federal de Telecomunicaciones y Radiodifusión, pandemias, sismos, etc.
- f) Para la identificación de los Factores de Riesgos las PSP se pueden apoyar en diversas herramientas como son diagramas de árbol de problemas o de Ishikawa, por mencionar algunos que nos permiten visualizar de forma gráfica las causas-efectos de un Riesgo a partir del análisis de una problemática.
- g) No confundir consecuencias con factores. Es muy frecuente que se establezcan como Factores de Riesgo situaciones como **incumplimiento a la normativa**, por lo que se deben establecer como Factores de Riesgo aquellas situaciones que pudieran propiciar el incumplimiento.

La definición de los tipos de Factores de Riesgo se muestra en la tabla siguiente:

TABLA 4. FACTORES DE RIESGOS

FACTORES INTERNOS	
HUMANO	Se relacionan con las actividades realizadas por las PSP que participan de manera directa o indirectamente en los proyectos, procesos y/o procedimientos. Asimismo, es atribuible a cambios en el personal, temas de capacitación, negligencia, capacidades para desempeñar funciones específicas.
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Se relacionan con los sistemas de información y comunicación automatizados; empleados para la operación de los proyectos, procesos y/o procedimientos.

METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS IFT

FINANCIERO-PRESUPUESTAL	Se refieren a la utilización de los recursos financieros y presupuestales necesarios para el logro de objetivos y metas de los proyectos, procesos y/o procedimientos.
TÉCNICO - ADMINISTRATIVO	Son actividades relacionadas con la planificación, organización, dirección y control de los recursos necesarios para la ejecución de los proyectos, procesos y/o procedimientos.
MATERIALES	Involucra situaciones que pudieran afectar la infraestructura y los recursos materiales que permiten la operación de los proyectos, procesos y/o procedimientos.
NORMATIVO	Cambios, desactualización en las leyes, reglamentos, normas y disposiciones que rigen la actuación del Instituto que pudieran afectar la ejecución de los proyectos, procesos y/o procedimientos.
DATOS PERSONALES	Actividades relacionadas directamente con el uso automatizado o no automatizados de información clasificada, reservada o con datos personales de terceros, de conformidad con lo establecido en el Art. 38 de la LGPDPSO; los cuales pueden ser: <ul style="list-style-type: none"> • Uso, acceso o tratamiento no autorizado • Robo, extravío o copia no autorizada • Daño, la alteración o modificación no autorizada • Pérdida o destrucción no autorizada
TELETRABAJO	<div> <div> Internos: <ul style="list-style-type: none"> • Organización • Infraestructura • Mecanismos de comunicación • Accesos remotos, etc. </div> <div> Externos: <ul style="list-style-type: none"> • Temas ambientales • Servicios de telecomunicación • Temas disciplinarios • Sociales y culturales, etc. </div> </div>
ENTORNO INTERNO	Conjunto de condiciones internas en el Instituto que inciden en el logro de los objetivos de las UA y de los proyectos, procesos y/o procedimientos sobre los cuales se ejerce influencia en el tramo de control correspondiente.

FACTORES EXTERNOS	
ENTORNO EXTERNO	Conjunto de condiciones externas al Instituto que inciden en el logro de los objetivos institucionales y de los proyectos, procesos y/o procedimientos, y sobre los cuales no se tiene influencia.
DESASTRES NATURALES	Referentes a situaciones provocadas por el medio ambiente y que detonan Riesgos críticos de continuidad de la operación en las institucionales, tales como: <ul style="list-style-type: none"> • Sismos • Incendios • Inundaciones • Pandemias • Ciclones y huracanes, etc.

Ejemplo de cómo analizar el entorno: En esta etapa es importante tomar en cuenta lo siguiente:

Analizar el entorno; es decir, las situaciones (ambiente y contexto) en las que se desarrollan las actividades del Instituto; así como, identificar los posibles obstáculos y áreas de oportunidad para evitarlos o mitigarlos y garantizar el logro del objetivo esperado; consiste en verificar todo lo que rodea o impacta a los proyectos, procesos y/o procedimientos, ya sea de forma interna o externa.

Algunas de las situaciones, a modo de ejemplo, que se deben tomar en consideración son las siguientes:

- Volumen de operaciones y datos
- Número de transacciones

- Áreas involucradas
- Personal capacitado
- Las actividades de supervisión empleadas.
- La normativa aplicable como: las atribuciones estatutarias, los manuales de operación empleados; leyes, reglamentos, códigos, etc.

Asimismo, es importante identificar las situaciones del entorno externo que pueden afectar el desarrollo del proyecto, proceso y/o procedimiento, por ejemplo:

- Cambios en la legislación aplicable.
- Eventos de seguridad pública.
- Condiciones sanitarias y medio ambientales.
- Fluctuaciones cambiarias.
- Escrutinio público y de medios de comunicación.

Este análisis proveerá de elementos suficientes para la identificación de los Factores de Riesgos que sean precursores de la materialización de un Riesgo.

Finalmente, en el análisis del entorno tanto interno como externo, es de suma importancia tomar en cuenta las situaciones que sucedieron en el pasado, así como aquellas que pueden ocurrir en un futuro cercano, sumando a las situaciones actuales por las cuales se desarrollan las actividades del Instituto. Con esto, tendremos a nuestro alcance un panorama ampliado de todo lo que puede suceder dentro y fuera de cada proyecto, proceso y/o procedimiento y que puede materializar el Riesgo.

En la identificación de Factores de Riesgo es importante que se identifique, tanto el tipo de factor, como su correcta clasificación, dependiendo de su naturaleza;

Ejemplo: Si se detecta que el personal carece de conocimientos especializados para el desarrollo de sus actividades, estamos ante un tema de "Capacitación" y es una situación interna de tipo humano que, de materializarse, puede impactar en el cumplimiento del objetivo, por lo que es indispensable contar con personal capacitado.

Con un sencillo análisis como el anterior podemos definir un Factor de Riesgo como:

Situación	Personal que participa en el proyecto, proceso y/o procedimiento, pero no cuenta con las capacidades suficientes para desarrollar sus actividades.
Interna o externa	Interno
De naturaleza	Humano

Tenemos entonces un Factor de Riesgo identificado, apoyándonos de lo mencionado en el apartado 6.3.

TIPO DE FACTOR	CLASIFICACIÓN DEL FACTOR	FACTOR O CAUSA IDENTIFICADA
Interno	Humano	Personal con capacitación insuficiente.

De esta manera podemos analizar todas las situaciones que se presentan o se han presentado en el desarrollo de las actividades e identificar los factores que materializan el Riesgo de éstas, con el objetivo de establecer las medidas de control que mitiguen dichos factores.

Recomendación. Una forma sencilla de identificar los diversos Factores de Riesgo, con base en el análisis del entorno, consiste en formularse la pregunta siguiente:

¿Qué situación sucedió, sucede o puede suceder, interna o externamente, que afecte el cumplimiento del objetivo del proyecto, proceso y/o procedimiento?

En la Matriz de Administración de Riesgos los Factores de Riesgo se integran en el campo “Factores Precursores del Riesgo”, como se puede ver en los ejemplos de Factores de Riesgos que, de forma enunciativa más no limitativa, se muestran a continuación:

EJEMPLOS DE FACTORES PRECURSORES DEL RIESGO			
1	NORMATIVO	INTERNO	FALTA DE NORMATIVA QUE REGULE EL PROCESO.
2	NORMATIVO	INTERNO	NORMATIVA QUE REGULA EL PROCESO DESACTUALIZADA.
3	TÉCNICO	INTERNO	INFORMACIÓN INCOMPLETA PARA DESARROLLO DE ACTIVIDADES.
4	HUMANO	INTERNO	CAPACITACIÓN INSUFICIENTE PARA EL PERSONAL.
5	HUMANO	INTERNO	SUPERVISIÓN INADECUADA DE LAS ACTIVIDADES.
6	TECNOLÓGICO	INTERNO	FALTA DE UN SISTEMA DE GESTIÓN DE RIESGOS.
7	ADMINISTRATIVO	INTERNO	INADECUADA PLANEACIÓN DE LAS ACTIVIDADES.
8	ADMINISTRATIVO	INTERNO	RECEPCIÓN DE INFORMACIÓN INTERNA FUERA DE PLAZO.

6.5 IDENTIFICACIÓN DE LOS POSIBLES IMPACTOS (CONSECUENCIAS) DE LOS RIESGOS

Es necesario diferenciar entre los factores de riesgo y los impactos por la materialización de un Riesgo, aunque no siempre es fácil delimitar la frontera entre ambas. Las causas definen el origen del Factor de Riesgo y permiten identificar la esencia de lo que se considera como factor y su clasificación (categoría), mientras que los impactos son las consecuencias o resultados que las causas producen y tienen la característica particular de afectar negativamente los objetivos de las UA y/o de los proyectos, procesos y/o procedimientos.

Se describirán los impactos por la materialización del Riesgo identificado, los cuales incidirán en el cumplimiento de los objetivos del IFT.

Tipos de Impactos o consecuencias:

- **Calidad de los servicios.** Reduce la calidad de los bienes y servicios que otorga el Instituto.
- **Imagen pública.** Afecta negativamente la imagen pública del Instituto.
- **Daño Patrimonial.** Afectación negativa en los recursos del Instituto.
- **Daño en los Procesos.** Demerita el desarrollo de los procesos sustantivos y adjetivos del instituto.

- **Metas financieras.** Impide el cumplimiento de metas financieras.
- **Objetivos y Estrategias Institucionales.** Dificulta el logro de los objetivos y estrategias del Instituto, así como, el cumplimiento de metas o el desempeño definidos en el Programa Anual de Trabajo del Instituto.
- **Satisfacción de los beneficiarios o usuarios.** Afecta el grado de satisfacción de los beneficiarios y usuarios de los servicios de Radiodifusión y Telecomunicaciones.
- **Incumplimiento de la normativa.** Afecta la capacidad de la institución para dar cumplimiento a la legislación y obligaciones contractuales.

6.6 ANÁLISIS Y EVALUACIÓN DE RIESGOS

El objetivo es determinar mediante un análisis de la información obtenida a partir de la identificación de los Factores de Riesgos, la Probabilidad de ocurrencia de un Riesgo y el nivel de Impacto de este sobre los fines que persigue el Instituto y su posible daño patrimonial, resultando en la evaluación, valoración y priorización de los Riesgos.

El análisis puede ser cualitativo, cuantitativo o una combinación de ambos y dependerá de los factores internos y externos; así como de la disponibilidad de datos e información.

La valoración en Probabilidad e Impacto de los Riesgos facilita la toma de decisiones, toda vez que permite determinar cuáles Riesgos necesitan acciones y la prioridad para implementarlas.

Para llevar a cabo la valoración de Riesgos, la diagramación de procesos es una herramienta que facilita la identificación y análisis de los Riesgos, en virtud de que presenta en forma gráfica la secuencia de actividades y permite delimitar las etapas y responsabilidades, así como, observar en forma conjunta un proyecto, proceso y/o procedimiento, así como la relación entre las actividades y los controles existentes.

Es importante mencionar que, para determinar la valoración de los Riesgos, se debe considerar la Probabilidad y el Impacto antes y después de la implementación de controles que ayuden a mitigarlos. Para ello se consideran las dos escalas que miden la Probabilidad de ocurrencia de los eventos y el Impacto sobre los objetivos determinados.

- **PROBABILIDAD DE OCURRENCIA:** Es la medida para estimar la posibilidad de que se materialice un Riesgo en un periodo determinado. Puede ser medida con criterios de frecuencia, teniendo en cuenta la presencia de factores tanto internos como externos.

La Probabilidad se mide con la escala siguiente:

Tabla 5. Probabilidad

ESCALA DE PROBABILIDAD		
VALOR	SEMÁFORO	DESCRIPCIÓN DEL GRADO DE PROBABILIDAD
10	RECURRENTE ALTO	Entre 91% y 100% de probabilidad de materialización del riesgo.
9	RECURRENTE	Entre 81% y 90% de probabilidad de materialización del riesgo.
8	MUY PROBABLE ALTO	Entre 71% y 80% de probabilidad de materialización del riesgo.
7	MUY PROBABLE	Entre 61% y 70% de probabilidad de materialización del riesgo.
6	PROBABLE ALTO	Entre 51% y 60% de probabilidad de materialización del riesgo.
5	PROBABLE	Entre 41% y 50% de probabilidad de materialización del riesgo.
4	POCO PROBABLE ALTO	Entre 31% y 40% de probabilidad de materialización del riesgo.

3	POCO PROBABLE	Entre 21% y 30% de probabilidad de materialización del riesgo.
2	REMOTO ALTO	Entre 11% y 20% de probabilidad de materialización del riesgo.
1	REMOTO	Entre 1% y 10% de probabilidad de materialización del riesgo.

- **IMPACTO SOBRE OBJETIVOS:** Se determina por la gravedad de las consecuencias o efectos negativos que puede ocasionar la materialización de un Riesgo en el logro de los objetivos de los proyectos, procesos y/o procedimientos del Instituto; lo cual se refleja en el incumplimiento de lo planeado.

Para indicar el porcentaje esperado de incumplimiento de objetivos, puede recurrirse a mediciones que se realicen expreso por cada proyecto, proceso y/o procedimiento (o métricas que ya se apliquen) respecto de lo que podría alcanzarse sin la implantación de controles que mitiguen o eviten los riesgos de no cumplir con los objetivos establecidos.

Ejemplo: Una UA del Instituto tiene planeado proporcionar 10 servicios en un periodo determinado; sin embargo, de acuerdo con la probabilidad de ocurrencia del proceso y sin aplicar controles adicionales, sólo cumpliría con 4; tendría un incumplimiento del 60%, lo cual ubica al riesgo con un valor o gravedad de 6, semáforo “Probable Alto”.

El Impacto se registra en la escala siguiente:

Tabla 6. Impacto

ESCALA DE IMPACTO		
VALOR (GRAVEDAD)	SEMÁFORO	% de incumplimiento de objetivos de proyectos, procesos y/o procedimientos
10	RECURRENTE ALTO	Entre 91% y 100% de incumplimiento.
9	RECURRENTE	Entre 81% y 90% de incumplimiento.
8	MUY PROBABLE ALTO	Entre 71% y 80% de incumplimiento.
7	MUY PROBABLE	Entre 61% y 70% de incumplimiento.
6	PROBABLE ALTO	Entre 51% y 60% de incumplimiento.
5	PROBABLE	Entre 41% y 50% de incumplimiento.
4	POCO PROBABLE ALTO	Entre 31% y 40% de incumplimiento.
3	POCO PROBABLE	Entre 21% y 30% de incumplimiento.
2	REMOTO ALTO	Entre 11% y 20% de incumplimiento.
1	REMOTO	Entre 1% y 10% de incumplimiento.

Es importante mencionar que, a mayor conocimiento de las consecuencias de la materialización del Riesgo, se contará con mejores elementos para determinar el nivel de Impacto.

Consideraciones: Apoyados en lo mencionado en el apartado 6.5, es necesario establecer una medida numérica de consecuencia sobre los objetivos, con base en la determinación de la Probabilidad de ocurrencia de un Riesgo en un periodo determinado (generalmente 12 meses calendario) y el Impacto de éste, sobre los objetivos de que se trate.

Recomendación: la valoración inicial del Riesgo se realiza previamente a considerar los controles implementados o por implementar.

En la Matriz de Administración de Riesgos; la valoración Inicial de la Probabilidad y el Impacto se integra en los campos "Probabilidad Inicial" e "Impacto Inicial" como se puede ver a continuación (incluye la consecuencia del Riesgo):

CONSECUENCIA DEL RIESGO	PROBABILIDAD INICIAL	IMPACTO INICIAL
<p>Recomendación. Una forma sencilla de identificar los diversos Factores de Riesgo, con base en el análisis del entorno, es formularse la siguiente pregunta:</p> <p>¿Qué pasa si se materializa el Riesgo?</p> <p>Algunos ejemplos de respuesta son;</p> <p>"Afectación directa a los objetivos establecidos en el Programa de Control Interno del IFT"</p> <p>"No alcanzar los objetivos Institucionales, la salvaguarda de los recursos públicos y la prevención de actos contrarios a la Integridad"</p> <p>"Se genera una inadecuada gestión de los Procesos por el incumplimiento de objetivos y metas."</p>	<p>Por ejemplo: 5</p> <p>"Establecer nivel de probabilidad Inicial alto"</p> <p>Recomendación. Una forma sencilla de identificar la Probabilidad antes de controles es formularse la siguiente pregunta:</p> <p>¿Qué tan probable que se materialice el Riesgo sin controles?</p>	<p>Por ejemplo: 5</p> <p>"Establecer nivel de Impacto Inicial alto"</p> <p>Recomendación. Una forma sencilla de identificar el impacto antes de controles es formularse la siguiente pregunta:</p> <p>¿Cuál es el impacto por la materialización del Riesgo sin controles?</p>

6.6.1 PRIORIZACIÓN INICIAL DE RIESGOS

Una vez realizada la valoración de la Probabilidad e Impacto, es necesario priorizar los Riesgos para determinar cuáles requieren de un tratamiento inmediato conforme a su ubicación en el Mapa Institucional de Riesgos, identificando la zona de riesgo que le corresponda de acuerdo con su evaluación.

TABLA 7. PRIORIZACIÓN 1
TABLA DE PRIORIZACIÓN INICIAL DEL RIESGO

NO. DE RIESGO	PROBABILIDAD INICIAL	IMPACTO INICIAL	VALOR DEL RIESGO*	PRIORIDAD DEL RIESGO	ORDEN JERÁRQUICO (PRIORIDAD)
42	10	9	9.50	MUY ALTO	1
32	8	7	7.50	ALTO	2
26	5	3	4.00	MEDIO	3
2	2	2	2.00	BAJO	4

* El Valor del Riesgo Inicial se obtiene de la suma de la ponderación del valor de la probabilidad al 50% y de la ponderación del valor del impacto al 50%.

La priorización de los Riesgos consiste en identificar aquellos Riesgos que requieren mayor atención en función de la Probabilidad de ocurrencia y del nivel de Impacto.

La escala para priorizar Riesgos se muestra a continuación y determina la gravedad del Riesgo de acuerdo con la Probabilidad e Impacto determinados al momento de la evaluación.

TABLA 8. PRIORIZACIÓN 2

SEMÁFORO DE PRIORIZACIÓN	ZONA DE RIESGO	ACCIÓN RECOMENDADA PARA ADMINISTRAR EL RIESGO
Riesgo grave (sector I riesgos de atención inmediata)	Zona de Riesgo significativo.	Tomar las acciones necesarias e inmediatas para mitigar los Riesgos que se encuentran en esta zona, es recomendable establecer un plan de prevención para tales fines.
Riesgo alto (sector II riesgos de atención periódica)	Zona de Riesgo alto.	Determinar acciones concretas y específicas a la brevedad posible para prevenir impactos graves en caso de materializarse el Riesgo debido a su alto grado de Probabilidad. Por otra parte, determinar si las acciones se comparten o transfieren a otras UA, de acuerdo con la naturaleza de cada acción.
Riesgo moderado (sector III riesgos de seguimiento)	Zona de Riesgo moderado.	Determinar las acciones permanentes y continuas necesarias para mitigar el Riesgo, considerando la posibilidad de compartirlas o transferirlas con otras UA de acuerdo con la naturaleza de cada acción.
Riesgo bajo (sector IV riesgos controlados)	Zona de Riesgo tolerable.	Determinar las acciones mínimas preventivas, detectivos o correctivas dependiendo de, si los Riesgos ubicados en esta zona se aceptan, previenen o mitigan.

Para mayor definición de cada uno de los sectores de priorización, se puede referir al apartado 11.2 “MAPA INSTITUCIONAL DE RIESGOS”.

7. IMPLEMENTACIÓN DE CONTROLES.

El establecimiento de controles que mitiguen los Factores de Riesgos identificados es de suma importancia, ya que éstos permiten la correcta administración y mitigación del Riesgo; asimismo, se debe privilegiar el diseño de los controles preventivos sobre los correctivos y detectivos.

Esta actividad es clave ya que la existencia de controles inadecuados o insuficientes manifiesta una administración de Riesgos deficiente, para lo cual, se debe realizar lo siguiente:

- Verificar la existencia de controles para los Factores de Riesgos identificados.
- Determinar el tipo de control que se ha implementado, ya sea preventivo, detectivo o correctivo, en el entendido de que los controles correctivos incrementan el costo de operación y los preventivos evitan incurrir en costos que sobrepasen los beneficios esperados.
- Identificar las características de los controles (actividades de control).

7.1 TIPOS DE CONTROLES.

- Preventivo:** Control que tiene el propósito de anticiparse a la posibilidad de que se materialice el Factor de Riesgo que pudiera afectar el logro de los objetivos del proyecto, proceso y/o procedimiento.

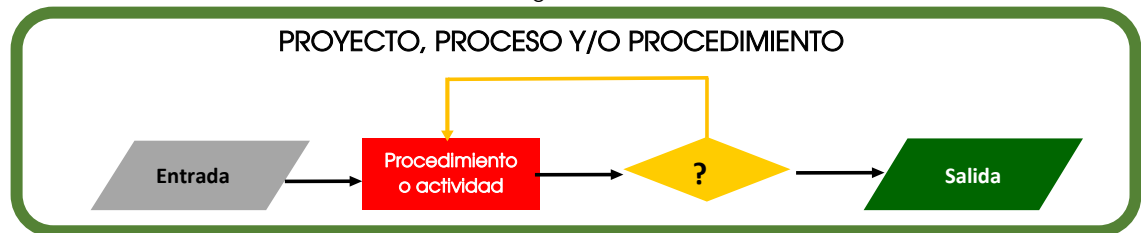
Figura 2



Esquema elaborado por el IFT

detectivo: Control que opera al momento en el que se están realizando las actividades e identifica las omisiones o desviaciones antes de que concluya el proyecto, proceso y/o procedimiento y permite anticiparse a la materialización del Riesgo que puede afectar el logro de objetivos.

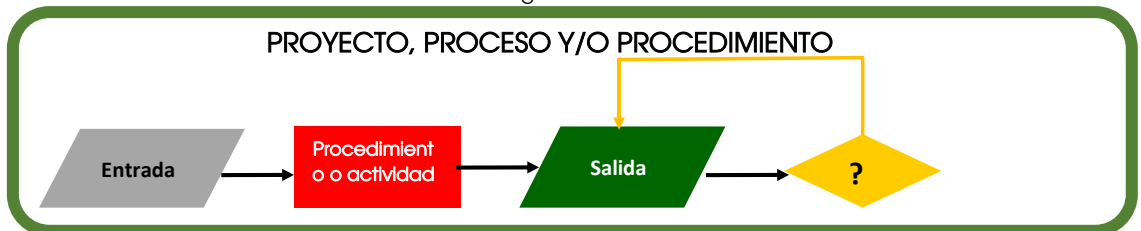
Figura 3



Esquema elaborado por el IFT

- **Correctivo:** Control que opera en la etapa final del proyecto, proceso y/o procedimiento, el cual permite identificar alguna omisión o desviación cuando posiblemente ya no se pueda corregir.

Figura 4



Esquema elaborado por el IFT

7.2 CARACTERÍSTICAS DE LOS CONTROLES.

En el diseño e implementación de los controles es importante considerar las características que éstos deben reunir para asegurar su eficiencia y efectividad, como las que se indican a continuación:

- Si es manual, semiautomático o automático.** El primer caso cuando corresponde a personas servidoras públicas realizarlo y generar evidencia; semiautomático, cuando además de las PSP también se involucre algún sistema automatizado y en el tercer caso es automático cuando sólo son ejecutados por sistemas informáticos y éstos generan de manera digital las evidencias correspondientes.

- b) **Frecuencia de ejecución:** El control debe ser planificado para ejercerse con determinada periodicidad la cual puede ser:
- Diaria
 - Semanal
 - Quincenal
 - Mensual
 - Trimestral
 - Semestral
 - Anual
 - Cuando se requiera
- c) **Evidencia de su ejecución.** Todo control debe proporcionar alguna evidencia de su ejecución, ya sea física o digital y, en su caso, dicha evidencia servirá de insumo para el análisis de la efectividad del control. Asimismo, las evidencias de la ejecución deben ser resguardadas por los Responsables de los proyectos, procesos y/o procedimientos, en el supuesto caso de alguna revisión por parte de cualquier órgano fiscalizador.
- d) **Estar documentados.** Deben encontrarse plasmados en la normatividad institucional y/o específica de las UA: Estatuto Orgánico, manuales de organización específicos, manuales de sistemas, de proyectos, de procesos y/o de procedimientos, de políticas, de prestación de servicios, etc.
- e) **Estar formalizados.** Deben encontrarse autorizados por las PSP que corresponda, de acuerdo con el ámbito de competencia y atribuciones.
- f) **Área responsable del control:** Es la Dirección General, Dirección General Adjunta o Dirección de Área encargada del diseño, implementación y aplicación del control, considerando que no en todos los casos puede coincidir con el Área de Riesgo.

7.3 EVALUACIÓN DE CONTROLES.

Una vez que se han identificado, evaluado y priorizado los Riesgos, es necesario revisar los controles que se han implementado en los proyectos, procesos y/o procedimientos para mitigar los riesgos; por ello es importante que, en diseño e implantación, se defina la obligatoriedad de ser evaluados al inicio de su ejecución y posteriormente de manera periódica, ya sea directa o indirectamente para asegurarse de su efectividad, en virtud de que cambios en el entorno interno y/o externo pueden debilitarlos o dejarlos sin efecto.

Como referencia, enunciativa más no limitativa, se presenta a continuación una guía de las características y elementos mínimos a observar en los controles que se implementen:

Verificación de controles	Descripción	Característica necesaria para considerar eficiente el control	
Establece frecuencia de ejecución	El control debe indicar la periodicidad de su ejecución; como puede ser: Diario, Semanal, Mensual, Trimestral, Semestral, Anual, Cuando se requiera u otra.	Sí	
Genera evidencia de ejecución	El control debe proporcionar evidencia documental (impresa o digital) de su ejecución.	Sí	
Cuenta con un diseño eficaz	El control debe ser diseñado atendiendo a las especificaciones particulares de cada proyecto, proceso y/o procedimiento, para que logre cumplir con su propósito	Sí	
Está documentado	El control debe estar descrito en documento oficial del Instituto.	Sí	
Está formalizado	El control debe estar formalizado en un documento aprobado, autorizado y firmado por autoridad competente, así como difundido oficialmente,	Si	

Los controles que cumplan con las especificaciones necesarias para considerarse eficaces garantizan la mitigación del factor de riesgo por lo que fueron implementados, ya que proceden de actividades reales, concretas y capaces de proporcionar evidencia documental y estadística para llevar la administración (monitoreo y vigilancia) del Riesgo.

Consideraciones:

Para cada Factor de Riesgos identificado se implemente por lo menos un control para mitigarlo.

A continuación, se enlistan los campos para identificar los controles implementados o por implementar y el tipo de información que requiere cada campo en la Matriz de Administración de Riesgos:

NÚMERO DE CONTROL	NOMBRE DEL CONTROL	CLASIFICACIÓN DEL CONTROL	FRECUENCIA DE EJECUCIÓN	TIPO DE CONTROL	EVIDENCIA DE LA EJECUCIÓN
1	Especificar de forma concreta y en pocas palabras, cómo se identifica al control.	Indicar si el control es:	Indicar la periodicidad para su ejecución.	Especificar si el control es:	Describir el documento o archivo generado por la ejecución del control.
	<p>Ejemplo:</p> <p>Informe de detección de necesidades de capacitación.</p> <p>El control debe de resolver la causa o situación identificada como Factor de Riesgo.</p>	<p>Manual (Si el control lo realizan PSP y NO se apoya de herramientas tecnológicas). Semiautomático. Si intervienen PSP y herramientas tecnológicas</p> <p>Automático Si el control se ejecuta exclusivamente con herramientas tecnológicas.</p>	<ul style="list-style-type: none"> • Diario • Mensual • Semanal • Semestral • Anual • Cuando se requiera • Otra 	<ul style="list-style-type: none"> • Preventivo • Detectivo o • Correctivo 	<p>Ejemplos:</p> <ul style="list-style-type: none"> • Informe del sistema SAPFIN • Constancias de capacitación • Estadística de encuestas aplicadas • Registros digitales contenidos en los sistemas de cómputo

A continuación, se enlistan los campos que permiten conocer las características de los controles implementados o por implementar por las UA y el tipo de información que requiere cada campo en la Matriz de Administración de Riesgos:

¿DISEÑO EFICAZ?	¿ESTÁ DOCUMENTADO?	¿ESTÁ FORMALIZADO?	¿SE APLICA?	¿CONSIDERAS QUE ES EFECTIVO?
<ul style="list-style-type: none"> • SÍ • NO 	<ul style="list-style-type: none"> • SÍ • NO 	<ul style="list-style-type: none"> • SÍ • NO 	<ul style="list-style-type: none"> • SÍ • NO 	<ul style="list-style-type: none"> • SÍ • NO
<p>Se considera que un control es eficaz cuando cumple con lo siguiente:</p> <ul style="list-style-type: none"> • Cuenta con tareas específicas para mitigar el Factor de Riesgo. 	<p>Se considera un control documentado cuando se integra en alguno de los siguientes:</p> <ul style="list-style-type: none"> • Mapeo del Proceso 	<p>Se considera un control formalizado, cuando el documento es debidamente autorizado y firmado por autoridad pertinente.</p>	<p>Se considera aplicado un control cuando se ejecuta periódicamente y se cuenta con los mecanismos para verificar su aplicación.</p>	<p>Se considera efectivo un control cuando cumple su función de mitigar el Factor de Riesgo por el cual fue diseñado.</p>

<ul style="list-style-type: none"> • Es ejecutado en un determinado momento dentro de las fases del proyecto, proceso y/o procedimiento • Proporciona una evidencia de su ejecución. • Determina la periodicidad de su ejecución y los responsables. 	<ul style="list-style-type: none"> • Narrativa del Proceso • Manuales de procedimiento • Políticas • Lineamientos • Circulares • Etc. 		Un control se puede aplicar sin documentar ni formalizar.	
---	---	--	---	--

En la Matriz de Administración de Riesgos, los controles se integran en los campos:

Numero de control, nombre de control, clasificación del control, frecuencia de ejecución, tipo de control y evidencia de ejecución, como se puede ver a continuación:

NÚMERO DE CONTROL	NOMBRE DEL CONTROL	CLASIFICACIÓN DEL CONTROL	FRECUENCIA DE EJECUCIÓN	TIPO DE CONTROL	EVIDENCIA DE LA EJECUCIÓN
1	Tablero de control Acciones PACII	Manual	Trimestral	Preventivo	Informe trimestral de acciones PACII

En la Matriz de Administración de Riesgos la evaluación de la efectividad de los controles se integra en los campos (campos preguntas):

¿Diseño adecuado?, ¿Está documentado?, ¿Está formalizado?, ¿Se aplica?, ¿Es efectivo?; como se puede ver a continuación:

¿DISEÑO EFICAZ?	¿ESTÁ DOCUMENTADO?	¿ESTÁ FORMALIZADO?	¿SE APLICA?	¿ES EFECTIVO?
Sí	Sí	Sí	Sí	Sí

8. VALORACIÓN FINAL DE RIESGOS RESPECTO A CONTROLES.

En esta etapa se realizará la confronta de los resultados de la evaluación de Riesgos y de controles, a fin de visualizar la máxima vulnerabilidad a que está expuesto el Instituto por no responder adecuadamente ante ellos, considerando los aspectos siguientes:

- La valoración final del Riesgo nunca podrá ser igual o superior a la valoración inicial, si se establecen controles para mitigar los Factores de Riesgo;
- La valoración final carecerá de validez cuando no considere la valoración inicial del Impacto y de la Probabilidad de ocurrencia del Riesgo, la totalidad de los controles existentes y su evaluación de controles.
- La valoración final indicará si fue posible alcanzar las metas establecidas en el diseño de los controles.

Tomando como referencia las escalas de valoración de la Probabilidad y el Impacto mencionadas en el apartado 6.6 "Análisis y Evaluación de Riesgos", se debe realizar una valoración final a los Riesgos, considerando la efectividad de los controles con base en sus características identificadas.

El resultado de la valoración final es el “RIESGO RESIDUAL”, el cual refleja el Riesgo remanente una vez que se han implementado de manera eficaz los controles por cada responsable para mitigar el Riesgo inherente.

En caso de que los controles establecidos no mitiguen los Factores de Riesgo, la valoración final podrá ser igual a la valoración del Riesgo inherente.

PRIORIZACIÓN DE LOS RIESGOS CON ALTO IMPACTO EN LA AFECTACIÓN DE LOS OBJETIVOS INSTITUCIONALES

Los riesgos que impidan directamente la consecución de los objetivos tanto institucionales, como de las UA y de sus proyectos, procesos y/o procedimientos alineados a la misión y visión del Instituto, deberán priorizarse, tomando acciones inmediatas para su mitigación o bien la pronta recuperación en la afectación a éstos; por lo que, los controles implementados por las PSP responsables serán puntuales y precisos orientados a mitigar el daño específico identificado para cada caso.

PRIORIZACIÓN DE LOS RIESGOS OPERATIVOS, CON AFECTACIÓN DE LOS OBJETIVOS DE LOS PROYECTOS, PROCESOS Y/O PROCEDIMIENTOS.

Los riesgos que impidan directamente la consecución de los objetivos establecidos para los proyectos, procesos y/o procedimientos, deberán ser priorizados de acuerdo con la afectación a la operación de éstos, por lo que la implementación de los controles debe considerar lo siguiente:

- La ubicación del riesgo en el mapa de riesgos.
- La gravedad esperada en la afectación a los objetivos.
- La pérdida patrimonial
- El posible incumplimiento normativo.
- La afectación a la continuidad de las actividades en los proyectos, procesos y/o procedimientos. Esto determinará la prontitud y exactitud con la que se debe diseñar e implementar un control; para así determinar el grado de prioridad que tendrá el riesgo residual.

Consideraciones:

Apoyados en lo mencionado en el apartado 8, es necesario establecer una medida numérica de consecuencia sobre los objetivos con base en determinar la Probabilidad de ocurrencia de un Riesgo en un periodo definido (generalmente 12 meses calendario) y el Impacto de éste, sobre el objetivo del proyecto, proceso y/o procedimiento.

Recomendación: La valoración final del Riesgo se realiza posterior a la implementación de los controles en el proyecto, proceso y/o procedimiento, considerando sus características y efectividad sobre la mitigación de los Factores de Riesgos por los cuales fueron diseñados.

En la Matriz de Administración de Riesgos la valoración Final de la Probabilidad y el Impacto se integra en los campos “Probabilidad final” e “Impacto final” como se puede ver a continuación:

PROBABILIDAD FINAL	IMPACTO FINAL
<p>Por ejemplo: 3</p> <p>"Establecer nivel de Probabilidad final bajo"</p> <p>Recomendación. Una forma sencilla de identificar la Probabilidad antes de controles es formularse la siguiente pregunta:</p> <p>¿Qué tan probable que se materialice el Riesgo después de implementar los controles?</p>	<p>Por ejemplo: 3</p> <p>"Establecer nivel de Impacto final bajo"</p> <p>Recomendación. Una forma sencilla de identificar el Impacto antes de controles es formularse la siguiente pregunta:</p> <p>¿Cuál es el Impacto por la materialización del Riesgo después de implementar los controles?</p>

8.1 PRIORIZACIÓN FINAL DE RIESGOS

Con el resultado de la suma ponderada se jerarquizan los Riesgos dentro de cada sector, ordenándolos de mayor a menor respecto al valor obtenido en la suma, como se muestra en el siguiente ejemplo:

TABLA 9. PRIORIZACIÓN 3
TABLA DE PRIORIZACIÓN DEL RIESGO

NO. DE RIESGO	PROBABILIDAD INICIAL	IMPACTO INICIAL	VALOR DEL RIESGO*	PRIORIDAD DEL RIESGO	ORDEN JERÁRQUICO (PRIORIDAD)
42	8	8	8.00	MUY ALTO	1
32	6	5	5.50	ALTO	2
26	3	3	3.00	MEDIO	3
2	1	1	1.00	BAJO	4

Tabla elaborada por el IFT.

* El Valor del Riesgo Final se obtiene de la suma de la ponderación del valor del impacto al 50% y de la ponderación del valor de la probabilidad al 50%.

9. TOLERANCIA AL RIESGO

La Tolerancia al Riesgo debe considerarse como el nivel aceptable de diferencia entre el cumplimiento cabal de los objetivos de las UA y de los proyectos, procesos y/o procedimientos, respecto de su grado real de cumplimiento.

El Titular de cada UA informará y comunicará al interior de sus respectivas unidades, los criterios de Tolerancia de los Riesgos de todo tipo (estratégicos, tecnológicos, operacionales, contrarios a la integridad, de afectación a la imagen, etc.), debiendo revisarlos al menos cada año o cuando se le requiera, con la finalidad de asegurar que se encuentran en niveles aceptables y que los controles implementados continúan siendo eficaces.

No obstante, en la determinación de la Tolerancia al Riesgo no debe existir tolerancia alguna para ningún caso, cuando se trate de los Riesgos de Actos Contrarios a la Integridad, así como para los que impliquen incumplimiento de cualquier disposición legal,

reglamentaria o administrativa relacionada con el servicio público, o que causen la suspensión o deficiencia de los servicios que proporciona el Instituto.

El Titular de cada UA instruirá la supervisión y monitoreo periódico, con la frecuencia establecida en el diseño de los controles, para asegurar que el comportamiento de los Riesgos se mantiene dentro de los niveles de tolerancia aceptables.

En caso de que la efectividad de los controles disminuya y los niveles de Riesgo excedan el criterio de tolerancia establecido, los Responsables de los proyectos, procesos y/o procedimientos, deberán informar al Titular de la UA inmediatamente después de haberlo detectado.

La Respuesta al Riesgo residual puede incluir políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos, es decir se ven reflejadas en actividades de control.

La decisión por parte de los Responsables de los proyectos, procesos y/o procedimientos respecto de implementar acciones para dar Respuesta al Riesgo residual debe estar sustentada en el marco normativo del Instituto y otros elementos que resulten aplicables. También se podrá tomar la decisión de no atender el Riesgo residual, lo que implica únicamente mantener los controles existentes operando efectivamente.

10. ESTABLECIMIENTO DE LA RESPUESTA AL RIESGO.

La Respuesta al Riesgo residual puede incluir políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos, es decir, se ven reflejadas en los controles (actividades de control) implementados por los Responsables de los proyectos, procesos y/o procedimientos.

La decisión por parte de los Responsables de los proyectos, procesos y/o procedimientos, de implementar o no de acciones para dar Respuesta al Riesgo residual, debe estar sustentada en el marco normativo del Instituto y en otros elementos que resulten aplicables. También se podrá tomar la decisión de no atender el Riesgo residual, lo que implica únicamente mantener los controles existentes operando efectivamente.

10.1 POLÍTICA DE RESPUESTA ANTE LA MATERIALIZACIÓN DEL RIESGO.

En esta etapa se debe tomar en cuenta el Mapa Institucional de Riesgos y la Tabla de Jerarquización del Riesgo para definir las acciones y estrategias, a efecto de responder ante la probable materialización del Riesgo identificado.

Con independencia del sector en el que se encuentren ubicados los riesgos (I, II, III y IV) se deben establecer acciones preferentemente preventivas, pudiendo optar por alguna de las estrategias siguientes:

- **Evitar el riesgo.** Se refiere a eliminar mediante controles efectivos, el factor o los factores que son precursores del Riesgo, realizando cambios sustanciales en el diseño de los procesos.
- **Reducir el riesgo.** Esta estrategia aplica cuando los Responsables de los proyectos, procesos y/o procedimientos, establecen acciones dirigidas a disminuir la probabilidad de ocurrencia y el nivel de impacto, tales como, la optimización de los procedimientos y la implementación de controles.

- **Transferir o Compartir el riesgo.** Implica que un tercero asuma de forma parcial o total la responsabilidad y la Administración del Riesgo; en los procesos en los que intervienen diversos actores es mayormente factible llevar a cabo esto, ya que cada uno asume el segmento que le corresponde, de acuerdo con el ámbito de su competencia.
- **Asumir el riesgo.** Si los Responsables de los proyectos, procesos y/o procedimientos, determinan que el Riesgo se encuentra en un nivel bajo (mínimo) de Impacto y Probabilidad remota de ocurrencia, pueden asumirlo en caso de que se presente la materialización de éste, sin necesidad de tomar otras medidas de control.

APLICACIÓN PRÁCTICA

Consideraciones: Para establecer la Respuesta al Riesgo, se debe considerar lo siguiente:

1. En el campo **"Respuesta al riesgo"**, determinar con base en la valoración de la efectividad de los controles implementados, una de las cuatro respuestas descritas en este numeral.
2. En el campo **"Acciones de respuesta"** se puede presentar alguna de las dos situaciones.

Opción 1 (sentido negativo). NO se estableció alguna estrategia; ya que los controles permiten asegurar el cumplimiento de los objetivos del proyecto, proceso y/o procedimiento; por lo tanto, no se determinan acciones de respuesta haciendo esta mención.

Nota 1. Si el Proceso ha cubierto su necesidad de implementar controles; entonces puede asumirse la Opción 1; por lo que no es necesario proseguir con los siguientes campos.

Opción 2 (sentido afirmativo). Se establecen controles nuevos para fortalecer los mecanismos de control existentes, con el propósito de mitigar el Riesgo.

Nota 2. Si por necesidad de apoyar a los controles implementados en el Proceso; es necesario asumir la Opción 2; entonces se prosigue con los siguientes campos.

3. En el campo **"Entregables de acciones implementadas"**, se deben detallar los documentos o entregables que se generarán por los nuevos controles, en caso de haber optado por la situación 2 del punto anterior.
4. En el campo **"Área responsable de la implementación"** se debe detallar el área o las áreas responsables de la implementación de los nuevos controles.
5. En el campo **"Fecha de implementación"** se debe indicar la fecha en la que se planea implementar los nuevos controles (basta señalar el año).

En la Matriz de Administración de Riesgos; la valoración final de la Probabilidad y el Impacto se integra en los campos "Probabilidad final" e "Impacto final" como se puede ver a continuación:

RESPUESTA AL RIESGO	ACCIONES DE RESPUESTA	ENTREGABLES DE ACCIONES IMPLEMENTADAS	ÁREA RESPONSABLE DE LA IMPLEMENTACIÓN	FECHA DE IMPLEMENTACIÓN
<p>Determinar solo una respuesta</p> <ul style="list-style-type: none"> • Evitar • Reducir • Transferir • Asumir 	<p>Ejemplo: La DCIAR contempla como estrategia para mitigar el Riesgo; la implementación de nuevos controles a partir de 2022:</p> <ul style="list-style-type: none"> • Establecer las reglas de operación del GTMCIAR. • Elaborar el Manual de Procedimientos de la DCIAR. • Elaborar la Solicitud de adquisición y/o desarrollo de sistemas. 	<p>Ejemplo: Las evidencias esperadas de las acciones de respuesta propuestas serán:</p> <ul style="list-style-type: none"> • Reglas de Operación del GTMCIAR • Manual de Procedimientos de la DCIAR • Formato de Adquisición y/o Formato de Desarrollo 	<p>Ejemplo: Dirección General de Finanzas, Presupuesto y Contabilidad</p>	<p>Ejemplo: Enero de 2025.</p>

11. HERRAMIENTAS PARA LA ADMINISTRACIÓN DE RIESGOS.

El proceso de Administración de Riesgos se apoya en diversas herramientas para registrar, analizar, evaluar, priorizar y dar respuesta a los Riesgos; tales herramientas tendrán como objetivo proporcionar una serie de acciones y mecanismos efectivos para que las UA visualicen el contexto general de los Riesgos a nivel proceso y demás niveles operativos, así como, la criticidad de cada Riesgo y el nivel de atención que deben tener, con el fin de implementar acciones para dar Respuesta al Riesgo y administrarlos de acuerdo con lo señalado en las Normas y la presente Metodología.

Las herramientas mínimas que deben emplearse en el proceso de Administración de Riesgos son:

- I. LA MATRIZ DE ADMINISTRACIÓN DE RIESGOS
- II. EL MAPA INSTITUCIONAL DE RIESGOS
- III. EL PROGRAMA ANUAL DE ADMINISTRACIÓN DE RIESGOS

11.1 MATRIZ DE ADMINISTRACIÓN DE RIESGOS.

Cada uno de los apartados anteriores, forman parte de la Matriz de Administración de Riesgos. Dicha Matriz constituye una herramienta de gestión de riesgos y permite a las UA documentar los proyectos, procesos y/o procedimientos, así como sus objetivos correlacionándolos con los riesgos que amenazan el logro de éstos; de esta forma, se determina el nivel de Riesgo, control y tipo de respuesta que requiere cada Riesgo.

La Matriz de Riesgo se divide en tres secciones:

- a) Sección I. Identificación de Riesgos
- b) Sección II. Controles implementados o establecidos
- c) Sección III. Respuesta al Riesgo

A continuación, se enlistan los elementos mínimos, más no limitativos, que debe contener la Matriz de Administración de Riesgos en cada sección:

Sección I. "Identificación de Riesgos"

- Número de riesgo
- Proceso
- Objetivo del Proceso
- Tipo de Proceso
- Nombre del Riesgo
- Descripción del Riesgo
- Tipo de Riesgo
- Clasificación del Riesgo
- Consecuencias del Riesgo
- Factores de Riesgo
- Área de riesgo
- Valoración inicial de Probabilidad
- Valoración inicial de Impacto
- Semáforo inicial de prioridad de riesgo.

Sección II. "Controles"

- Número de control
- Nombre del control
- Tipo de control
- Frecuencia de ejecución
- Área responsable del control
- Evidencia de ejecución
- Características del control
- Valoración final de Probabilidad
- Valoración final de Impacto
- Semáforo final de prioridad de riesgo.

Sección III. "Respuesta al Riesgo"

- Número de control
- Respuesta al Riesgo (evitar, reducir, transferir, asumir)
- Acciones de respuesta
- Entregables de acciones implementadas
- Área responsable de la implementación
- Fecha de implementación

11.2 MAPA INSTITUCIONAL DE RIESGOS.

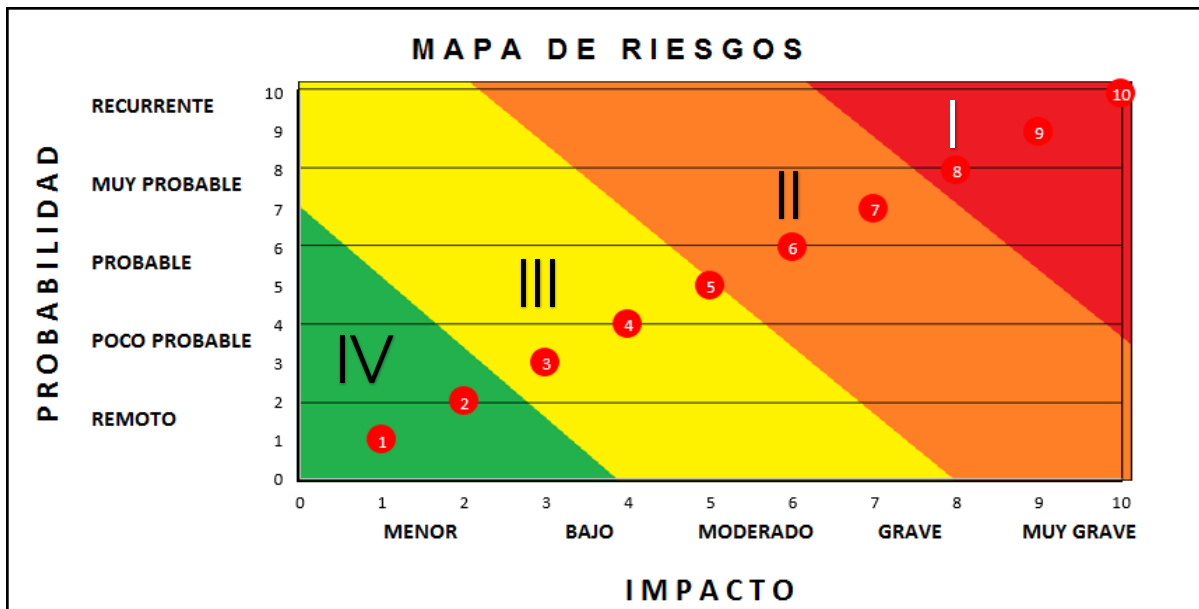
Es la representación gráfica del conjunto de Riesgos priorizados o jerarquizados, que vincula tanto la Probabilidad de ocurrencia de los riesgos y su nivel de Impacto sobre los objetivos del Instituto, así como de los proyectos, procesos y/o procedimientos.

Los Riesgos se ubican por sectores y se grafican en el **Mapa Institucional de Riesgos**, en función del Impacto y la Probabilidad de ocurrencia de manera posterior a la valuación de la efectividad de las actividades de control.

El grado de priorización o atención a los Riesgos depende de su ubicación dentro de los cuatro sectores del Mapa Institucional de Riesgos, como se observa a continuación:

- **Sector I. Riesgos de Atención Inmediata.**
- **Sector II. Riesgos de Atención Periódica.**
- **Sector III. Riesgos de Seguimiento.**
- **Sector IV. Riesgos Controlados.**

Figura 5

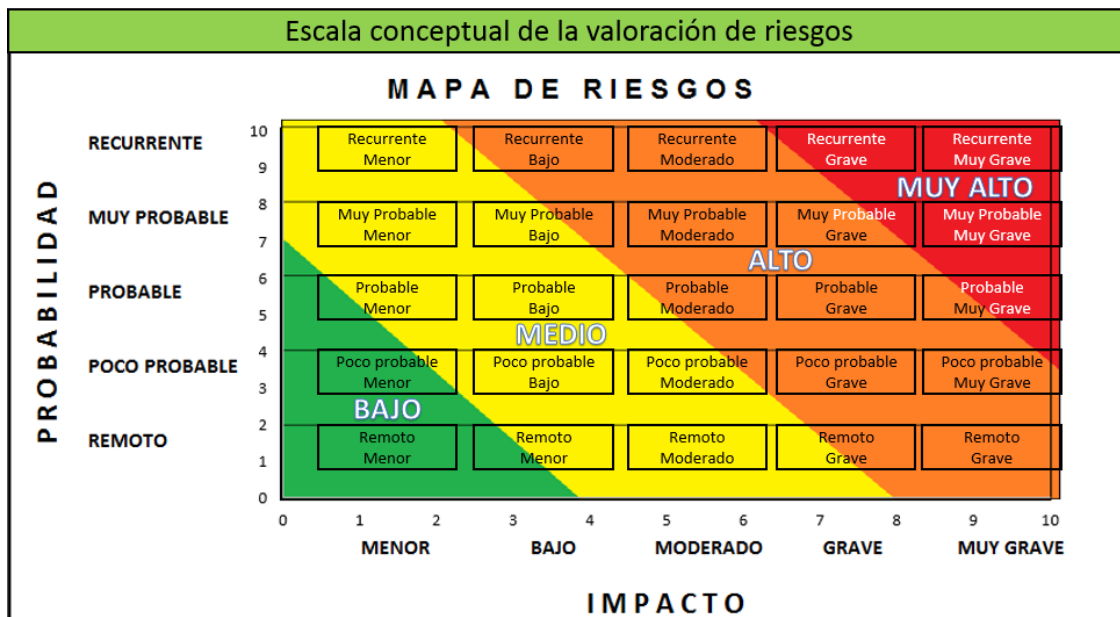


Mapa elaborado por el IFT

La posición de los Riesgos en los sectores (I, II, III y IV) identifica las prioridades para determinar cuáles necesitan acciones inmediatas para su atención y administración, conforme al apartado 6.6.1 "Priorización de Riesgos".

Lo anterior corresponde al siguiente esquema:

Figura 6



Mapa elaborado por el IFT

El Mapa Institucional de Riesgos se interpreta de la siguiente manera:

- **Sector I. Riesgos de Atención Inmediata.** – Se consideran muy graves por su alta Probabilidad de ocurrencia y nivel de impacto, ya que al materializarse pueden impedir el cumplimiento de los objetivos institucionales; éstos deben ser reducidos o administrados con controles preventivos y detectivos con énfasis en los primeros.
- **Sector II. Riesgos de Atención Periódica.** – Se consideran como graves por su alta Probabilidad de ocurrencia. Estos Riesgos al igual que los ubicados en el sector I, son relevantes para el logro de los objetivos, por lo que deben recibir una alta prioridad y deben ser atendidos con actividades de control preventivas.
- **Sector III. Riesgos de Seguimiento.** – Éstos son considerados como moderados por su nivel de Impacto. Los Riesgos que se encuentren en este sector deben ser administrados correctamente de manera permanente y continua, asegurándose que las modificaciones de las condiciones internas y externas no han modificado su probabilidad de ocurrencia.
- **Sector IV. Riesgos Controlados.** – Están considerados como Riesgos con Probabilidad e Impacto bajos sobre los objetivos y requieren de un seguimiento mínimo, a menos de que una evaluación de Riesgos posterior muestre un cambio sustancial y éstos se trasladen hacia un sector de mayor Impacto y Probabilidad de ocurrencia.

Por otra parte, para los Riesgos identificados en el sector IV, se recomienda establecer acciones preventivas, así como, mantenerlos monitoreados y supervisarlos al menos una vez al año.

El Mapa Institucional de Riesgos es una importante herramienta que proporciona información útil para valorar los Riesgos en su conjunto, y definir las estrategias que permitan al Instituto la adecuada administración de éstos.

11.3 EL PROGRAMA ANUAL DE ADMINISTRACIÓN DE RIESGOS (PAAR)

De conformidad con las Normas, para dar seguimiento a la implementación de los controles y estrategias establecidas en la Matriz de Administración de Riesgos, el PAAR será elaborado por la DGFPD y revisado por el Titular de la UADM, quien lo presentará al Comisionado Presidente para su aprobación. Con este programa se dará seguimiento a la implementación de los controles y estrategias establecidas por las UA en su Matriz de Administración de Riesgos, así como de aquellas acciones inconclusas programadas en el PAAR del ejercicio fiscal anterior; tendrá una periodicidad anual y considerará los apartados que se establecen en el artículo 18 de las Normas.

En su caso, se podrán incorporar las recomendaciones emitidas por los órganos fiscalizadores, evaluadores internos y externos y las que instruya el Comisionado Presidente.

El mecanismo de seguimiento será mediante un reporte trimestral, elaborado por la DGFPD en coordinación con las UA; el cual referirá el avance en la ejecución de los controles implementados; así como, la programación de los controles por aplicar a futuro y demás acciones a realizar y la descripción de la problemática principal que puede obstaculizar su cumplimiento. La difusión se realizará por medios institucionales a las personas servidoras públicas del Instituto.

La evidencia documental y/o electrónica que acredite la implementación y avances reportados, será resguardada por las PSP responsables de las acciones de control

comprometidas en el PAAR y deberá ponerse a disposición de la DGFPC cuando así lo requiera, a efecto de constatar que la evidencia soporta el cumplimiento de las acciones.

11.4 FORMALIZACIÓN DE LA MATRIZ DE ADMINISTRACIÓN DE RIESGOS Y EL MAPA INSTITUCIONAL DE RIESGOS

Tanto la Matriz de Administración de Riesgos, como el Mapa Institucional de Riesgos deben ser del interés de todas las PSP del Instituto; por ello, la importancia de dar a conocer los resultados del proceso de Administración de Riesgos, a efecto de que sean plenamente conocidos, tanto por los Responsables de los proyectos, procesos y/o procedimientos, como por las máximas autoridades.

En ese contexto, una vez terminado el proceso de Administración de Riesgos, la Matriz de Administración de Riesgos junto con el Mapa Institucional de Riesgos, deben ser formalizados mediante FEDI (cuando menos) por las PSP siguientes:

- a) El Titular de la Unidad Administrativa.
- b) La Dirección General o Dirección General Adjunta del área correspondiente a cada Matriz de Administración de Riesgos.
- c) La DGFPC como responsable del SCII.

Por otra parte, según sea el caso, podrán participar de manera opcional en la formalización de la Matriz de Administración de Riesgos las PSP siguientes:

- a) La PSP que coordinó la elaboración de la matriz por cada UA o en su defecto, apoyo en la integración de la información por parte de la UA;
- b) La Dirección de Control Interno y Administración de Riesgos.

Será responsabilidad de este último, coordinar los esfuerzos con los Titulares de las UA para difundir la Matriz de Administración de Riesgos y el Mapa Institucional de Riesgos a todos los niveles del Instituto, con apoyo del GTMCIAR.

12. INFORMACIÓN Y COMUNICACIÓN

En esta etapa se procede a informar los resultados más relevantes a todas las PSP, conforme a los principios del componente de Información y Comunicación que establecen las Normas, como se describe a continuación:

- Los resultados relevantes se comunicarán a las UA mediante los Enlaces del GTMCIAR que define el artículo 6, numeral IV de las Normas.
- Se presentará la Matriz de Administración de Riesgos al Titular de la UA con el objetivo de que éste determine las acciones correspondientes para la Administración de Riesgos.
- Los resultados del proceso de Administración de Riesgos deberán informarse al Comisionado Presidente en el Informe Anual del Estado que Guarda el SCII.

13. SUPERVISIÓN

En esta etapa los Responsables de los proyectos, procesos y/o procedimientos supervisarán, con el apoyo de la DGFP, la correcta Administración de Riesgos, de conformidad con los principios del componente de Supervisión que establecen las Normas.

- a) Supervisar los controles implementados en su Unidad Administrativa, para verificar su adecuado funcionamiento y, en su caso, implementar las mejoras que se determinen.
- b) Reportar oportunamente en sus distintos niveles las debilidades de control identificadas e implementar, en su caso, las medidas que se determinen para su debida atención.

EL COMISIONADO PRESIDENTE DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES, con fundamento en los artículos 19, 20, fracciones III y XV, de la Ley Federal de Telecomunicaciones y Radiodifusión; 4, fracción II, y 14, fracción IV, del Estatuto Orgánico y 7, fracción IV, de las Normas de Control Interno del Instituto Federal de Telecomunicaciones, emite el siguiente:

ACUERDO

ÚNICO. Se aprueba la Metodología de Administración de Riesgos del Instituto Federal de Telecomunicaciones.

TRANSITORIOS

Primero. La presente Metodología entrará en vigor a partir del día siguiente de su aprobación por parte del Comisionado Presidente del Instituto.

Segundo. Se instruye a la Unidad de Administración del Instituto Federal de Telecomunicaciones, a publicar en la Intranet del Instituto Federal de Telecomunicaciones la presente Metodología al día siguiente de la aprobación del presente Acuerdo.

Tercero. La Metodología aprobada el 19 de diciembre de 2022, quedará sin efectos a partir de la entrada en vigor de la presente Metodología de Administración de Riesgos del Instituto Federal de Telecomunicaciones emitida mediante el presente Acuerdo.

Aprobó

JAVIER JUÁREZ MOJICA
COMISIONADO PRESIDENTE EN SUPLENCIA DEL
INSTITUTO FEDERAL DE TELECOMUNICACIONES*

Se firma electrónicamente

* En suplencia por ausencia del Comisionado Presidente del Instituto Federal de Telecomunicaciones, suscribe el Comisionado Javier Juárez Mojica, con fundamento en el artículo 19 de la Ley Federal de Telecomunicaciones y Radiodifusión.

