MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO

DIAN

Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN

Versión 2 - 03 de octubre de 2023

Subdirección de Procesos
Dirección de Gestión Estratégica y Analítica

Dirección de Gestión Estratégica y de Analítica
Carrera 8 #6C-38. Piso 4. Edificio San Agustín | 6017428973 - 3103158107
Código postal 111711
www.dian.gov.co
Formule su petición, queja, sugerencia o reclamo en el Sistema PQSR de la DIAN

Tabla de contenido

INTRODUCCIÓN

La UAE DIAN adelanta la administración de sus riesgos mediante el desarrollo de los siguientes sistemas:

- Sistema de Gestión de Riesgos Tributarios, Aduaneros y Cambiarios - Cumplimiento TAC.
- Sistema de Gestión de Riesgos Institucionales.

Como parte del Sistema de Gestión de Riesgos Institucionales y su despliegue, este documento contiene la política para su administración, la cual, incluye la declaración, compromiso y lineamientos integrales frente a la gestión de los riesgos institucionales en todos los niveles de su operación, que permiten direccionar las estrategias y acciones oportunas para evitar la materialización de los riesgos o reducir las vulnerabilidades o posibles consecuencias negativas a las que pueda estar expuesta la entidad, enmarcado en el cumplimiento de su misión y sus objetivos estratégicos.

Así mismo, la política contenida en el presente documento contempla el alcance, objetivo, los principios, la responsabilidad y autoridad frente a la gestión de los riegos institucionales, la metodología y niveles de aceptación del riesgo de acuerdo con tipo de riesgo, y los términos y definiciones.

Esta política está desarrollada teniendo en cuenta lo definido en el Modelo Integrado de Planeación y Gestión – MIPG, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP y la Norma NTC ISO 31000 de Gestión del Riesgo; y en concordancia con el Código de buen gobierno y la Política de Integridad de la entidad.

El despliegue del Sistema de Gestión de Riesgos Tributarios, Aduaneros y Cambiarios - Cumplimiento TAC se abordará en la política y normativas que se contemplen y lideren desde la Subdirección de Análisis de Riesgo y Programas.

1. DECLARACIÓN Y COMPROMISO DE LA UAE DIAN FRENTE AL SISTEMA DE GESTIÓN DE RIESGOS INSTITUCIONALES

En la UAE DIAN se administran de manera objetiva, integral, participativa y dinámica los siguientes riesgos institucionales:

- Riesgos estratégicos.
- Riesgos operacionales.
- Riesgos de capital humano.
- Riesgos de seguridad y salud en el trabajo.
- Riesgos ambientales.
- Riesgos de seguridad de la información.
- Riesgos de fraude y corrupción.
- Riesgos fiscales.

Para la efectiva y oportuna administración de estos riesgos, se asignan los recursos necesarios y se cuenta con el capital humano calificado, dispuestos a mitigar los niveles de incertidumbre asociados al cumplimiento de los objetivos institucionales y asegurar la continuidad del negocio.

En la entidad se asume de forma sistemática la gestión de los riesgos institucionales para lo cual se parte del análisis del contexto estratégico como base para la toma de decisiones, se realiza la identificación, la valoración de los riesgos y el establecimiento de controles o acciones oportunas que permitan la prevención o mitigación de afectaciones en las personas, procesos, activos, ambiente y demás recursos requeridos para su operación o prestación de servicios.

Así mismo, la UAE DIAN se compromete a gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo cualquier daño sobre éstos.

2. OBJETIVO

Establecer un enfoque integral para la gestión de los riesgos institucionales que permitan su prevención y control en todos los procesos, mediante la implementación de acciones tendientes a lograr un nivel de aceptación del riesgo acorde con los objetivos de la UAE DIAN, el cumplimiento normativo y las buenas prácticas aplicables.

3. ALCANCE

Aplica para todos los procesos, niveles de operación y prestación de servicios de la entidad, conforme a la responsabilidad y autoridad definida de acuerdo con cada tipo de riesgo y líneas de defensa.

4. PRINCIPIOS

Los principios fundamentales en los que se basa el Sistema de Gestión de Riesgos Institucionales y que orientan su actuación frente a los efectos de la incertidumbre en el cumplimiento de sus objetivos, son los establecidos en la norma NTC-ISO 31000:2018:

- **Integralidad**: La gestión del riesgo es parte integral de todas las actividades de la organización.

- **Estructurada y exhaustiva**: Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

- **Adaptada**: El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.

- **Inclusiva**: La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.

- **Dinámica**: Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.

- **Mejor información disponible**: Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas, es decir, los objetivos estratégicos o de mejoramiento de la gestión que establezca la entidad y/o el proceso. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.

- **Capital humano:** Promover el desarrollo integral y el bienestar de nuestro capital humano, reconociendo su valor como activo estratégico de la entidad.

- **Factores culturales:** Valorar y respetar la diversidad cultural como una fuente de enriquecimiento y crecimiento para la entidad.

- **Mejora continua**: La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

La gestión de riesgos de seguridad de la información, acoge y establece sus actividades basadas en los principios de la norma NTC-ISO/IEC 27001:2022, en los que se fundamentan el Modelo de Seguridad y Privacidad de la Información – MSPI/DIAN y el sistema de gestión de seguridad de la información de la entidad; adoptando los lineamientos y buenas prácticas para la gestión de ciberseguridad, privacidad y protección de datos personales con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información en los activos de la entidad.

5. RESPONSABILIDAD Y AUTORIDAD

Las responsabilidades y autoridad frente al Sistema de Gestión de Riesgos Institucionales se establece de acuerdo con las respectivas líneas de defensa aplicables en todos los niveles de la organización, en el marco de las funciones establecidas para la entidad a través del Decreto 1742 de 2020, la Resolución 000021 de 2022 y demás reglamentación aplicable vigente o aquella normativa que los sustituya o modifique, y en concordancia con lo definido en el Modelo Integrado de Planeación y Gestión – MIPG, Resolución Modelo de Gobernanza de Procesos y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP vigentes.

El Sistema de Gestión de Riesgos Institucionales es coordinado a través de la Dirección de Gestión Estratégica y de Analítica y la Subdirección de Procesos o las áreas que hagan sus veces, junto con los responsables metodológicos por tipo de riesgo institucional, quienes gestionan con los responsables de los procesos y sus equipos de trabajo, la identificación, valoración, monitoreo de los riesgos e implementación de mejoras o tratamientos en los diferentes niveles de la entidad para su prevención o control respectivamente.

Los responsables metodológicos por cada tipo de riesgo institucional son las siguientes dependencias:

Tabla 1. Responsables metodológicos por tipo de riesgo institucional

Riesgos Institucionales	
Tipo de riesgo	**Responsable**
Riesgos estratégicos.	Subdirección de Planeación.
Riesgos operacionales, ambientales y riesgos fiscales.	Subdirección de Procesos.
Riesgos de fraude y corrupción.	Subdirección de Procesos con el apoyo del área responsable de Transparencia o de quien haga sus veces.
Riesgos de seguridad de la información, incluyen riesgos de ciberseguridad y protección de datos personales.	Oficina de Seguridad de la Información.
Riesgos de Capital humano.	Dirección de Gestión Corporativa.
Riesgos de seguridad y salud en el trabajo.	Subdirección de Desarrollo de Talento Humano.

A continuación, se establece los niveles de responsabilidad y autoridad frente a la gestión de riesgos institucionales acorde con el esquema de líneas de defensa establecido en la entidad:

Tabla 2. Responsabilidad y autoridad frente a la gestión de riesgos

Línea de defensa	Responsable	Responsabilidad e instancia o nivel
Línea Estratégica	Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno Comité Institucional Estratégico - CIE o las instancias que hagan sus veces	En el marco del **Comité Institucional de Gestión y Desempeño:** • Definir lineamientos estratégicos para la administración del Sistema de Gestión de Riesgos Institucionales incluyendo lo asociado a continuidad de negocio y asegurar su implementación, seguimiento y mejora. En el marco del **Comité Institucional de Coordinación de Control Interno:** • Definir y aprobar la Política de administración de Gestión de Riesgos Institucionales, la cual se debe evaluar, considerando los análisis del entorno, alcance y objetivos que puedan generar cambios, así mismo, se debe facilitar su despliegue y entendimiento en todos los niveles de la Entidad. • Los responsables metodológicos de los diferentes tipos de riesgos institucionales deben presentar el seguimiento, mostrando lo más relevante, los riesgos críticos y situaciones que requieren intervención prioritaria. Con base en estos informes consolidados por la Subdirección de Procesos, y de la retroalimentación de la tercera línea, se debe realizar un análisis y tomar las acciones de mejora necesarias para enfrentar situaciones detectadas que pueden afectar el cumplimiento de los objetivos estratégicos, metas, prestación del servicio y la continuidad del negocio. En el marco del **Comité Institucional Estratégico -CIE** o la instancia que haga sus veces para la gestión de riesgos de seguridad de la información: • Aprobar y garantizar la aplicación de los protocolos para el manejo de crisis y emergencias. • Aprobar los riesgos de seguridad de la información que se encuentren fuera del apetito de riesgos. • Manejar situaciones en donde se identifique una negación en la implementación de las actividades incluidas en la metodología para la gestión de riesgos de seguridad de la información. • Definir las medidas que se deben tomar frente a desviaciones que afecten el desarrollo de la metodología de gestión de riesgos de seguridad de la información.

Línea de defensa	Responsable	Responsabilidad e instancia o nivel
1ª línea de defensa	**Líderes de los procesos** Subdirectores Jefes de Oficina Defensor del Contribuyente y del Usuario Aduanero y Cambiario o quienes hagan sus veces, según aplique.	• Participar en la implementación y mejora continua del Sistema de Gestión de Riesgos Institucionales; trabajando en colaboración con las demás líneas de defensas para gestionar adecuadamente los riesgos. • Liderar y participar en la identificación, valoración, monitoreo, seguimiento y tratamiento de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales, planes, proyectos y procesos. • Coordinar la actualización de las matrices de riesgos en caso de que se requiera, asignando los responsables de participar en dicha actualización. Así mismo, garantizar la divulgación y entendimiento en los distintos niveles de la entidad. • Realizar monitoreo y seguimiento permanente a la ejecución de los controles definidos para la gestión de los riesgos. Evaluar la pertinencia y efectividad de éstos. • Realizar seguimiento a las materializaciones de riesgos que se presenten, garantizando que se formulen y ejecuten acciones o planes de mejoramiento si se requieren, de forma oportuna, y según corresponda a la tipología del riesgo. • Presentar los informes de monitoreo de gestión de riesgos de acuerdo con la periodicidad e instancias definidas según el tipo de riesgo y retroalimentar a los dueños de los macroprocesos (Director de Gestión o quien haga sus veces). • Participar activamente en las auditorías internas, seguimientos por parte de la segunda y tercera línea de defensa o auditorías externas relacionadas con la gestión de los riesgos según aplique. • Definir los enlaces de riesgos para apoyar la gestión, los seguimientos, reportes y sensibilizaciones requeridas, según aplique. • Definir los expertos del proceso para apoyar la identificación y actualización de los riesgos asociados a los escenarios de continuidad del negocio. • Los responsables de los procesos deben administrar los recursos (físicos, financieros, talento humano, entre otros) que sean requeridos para implementar los controles necesarios y evitar que se materialicen los riesgos.
	Servidores públicos de los procesos Responsables de los proyectos	• Todos los servidores públicos son responsables de la ejecución de los controles y de reportar de forma oportuna los riesgos que se materialicen en los procesos. Así mismo, son responsables de proponer acciones de mejora en la gestión de riesgos, según corresponda. • El responsable del proyecto debe realizar la identificación de los riesgos y monitoreo a los controles definidos en el proyecto acorde a la estructura establecida, de igual manera deberá realizar el seguimiento a la implementación de acciones de mejora o prácticas que contribuyan a la gestión del riesgo durante la ejecución del proyecto.

Línea de defensa	Responsable	Responsabilidad e instancia o nivel
2ª línea de defensa	Responsables metodológicos por tipo de riesgo institucional (Tabla 1)	La dependencia responsable metodológica por cada tipo de riesgo institucional es responsable de lo siguiente: • Orientar y acompañar a los líderes de los procesos y sus equipos en la planificación, implementación, monitoreo y mejora de la gestión de riesgos institucionales, lo cual, incluye la definición de la metodología a utilizar, su revisión, actualización y desarrollo, teniendo como base las guías, normas y demás documentos aplicables a la entidad y al tipo de riesgo, teniendo en cuenta las siguientes responsabilidades: - Oficina de Seguridad de la Información. Es responsable de la orientación frente a los riesgos de seguridad de la información, los cuales incluyen los riesgos de ciberseguridad y protección de datos personales. - Dirección de Gestión Corporativa. Es responsable de la orientación frente a los riesgos de Capital humano. - Subdirección de Desarrollo de Talento Humano. Es responsable de la orientación frente a los riesgos de seguridad y salud en el trabajo. - Subdirección de Procesos. Es responsable de la orientación frente a los riesgos operacionales, ambientales, riesgos fiscales; y con el apoyo del Oficial de Transparencia son responsables de la orientación frente a los riesgos de fraude y corrupción. - Subdirección de Planeación y Cumplimiento. Es responsable de la orientación frente a los riesgos estratégicos. • Asesorar y acompañar a la primera línea de defensa en la identificación, valoración, monitoreo, seguimiento y tratamiento de los riesgos, según corresponda. • Realizar y/o apoyar actividades para fortalecer el entendimiento de la gestión de riesgos, tales como sensibilizaciones, capacitaciones, entre otros, según corresponda. • Realizar seguimiento periódico a los riesgos y controles aplicados por la primera línea de defensa, según corresponda, permitiendo que se generen alertas y orientaciones que conlleven al análisis y establecimiento de posibles mejoras por parte de la primera línea de defensa y la línea estratégica. • Implementar actividades de control específicas que permitan el seguimiento a la gestión de riesgos según aplique al tipo de riesgo, como puede ser la elaboración de informes, la realización de auditorías internas o externas, la evaluación y monitoreo al cumplimiento normativo, entre otros.

Línea de defensa	Responsable	Responsabilidad e instancia o nivel
3ª línea de defensa	Oficina de Control Interno	• Realizar la evaluación (aseguramiento) independiente sobre la gestión de los riesgos institucionales según aplique. Informar los hallazgos y proporcionar recomendaciones a la Línea Estratégica. • Evaluar y verificar que la gestión de riesgos se desarrolla de acuerdo con los lineamientos, políticas y procedimientos definidos para la Entidad. • Establecer la efectividad de los controles para evitar la materialización de riesgos. • Apoyar y asesorar en la gestión de riesgos según se requiera.

6. METODOLOGÍAS POR TIPO DE RIESGO

En el marco del modelo Integrado de Planeación y Gestión – MIPG, la Norma NTC ISO 31000 de Gestión del Riesgo, y de acuerdo con los tipos de riesgos, se ha establecido que, para su identificación, valoración, diseño e implementación de controles, monitoreo y seguimiento, se tendrán en cuenta las siguientes disposiciones:

Para la identificación de los riesgos se debe considerar la Planeación Estratégica de la entidad, con el respectivo análisis del entorno en el que opera y que pueden generar riesgos que afecten el cumplimiento de sus objetivos institucionales. Este contexto, incluye el análisis externo e interno.

Dependiendo del tipo de riesgo, y en concordancia con la gestión por procesos de la entidad, se cuenta con la documentación específica que establece la metodología aplicable y su desarrollo, incluyendo los niveles de calificación de probabilidad e impacto, acorde a lo siguiente:

a) Riesgos estratégicos, operacionales, ambientales, fiscales, fraude y corrupción y capital humano

La metodología para identificar, valorar, monitorear y hacer seguimiento a los riesgos estratégicos, operacionales, ambientales, fiscales, de fraude y corrupción y de capital humano se basa en los lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP, así mismo, en los lineamientos establecidos por la norma NTC ISO 14001:2015 Sistemas de Gestión Ambiental para los riesgos ambientales, los lineamientos de la Secretaría de Transparencia de la Presidencia de la República para el caso de los riesgos de fraude y corrupción, los lineamientos definidos en la

herramienta TADAT 2019 - Herramienta para el diagnóstico y evaluación de la administración tributaria para los riesgos de capital humano y los lineamientos definidos por la Subdirección de Planeación y Cumplimiento para el caso de los riesgos estratégicos.

b) Riesgos de seguridad de la Información

La metodología para la gestión de riesgos de seguridad de la Información está basada en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP y en el Anexo Técnico 4 - Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, versión 4 de octubre de 2021 del MinTic.

Así mismo, la metodología de gestión de riesgos de seguridad de la información determina que los siguientes son los criterios para iniciar una evaluación de riesgos de seguridad de la información en la entidad:

- Cuando se presente un requerimiento especifico de seguridad de la información de una entidad que regule a la UAE-DIAN.
- Cuando se presente un evento que esté relacionado con el Sistema de Gestión de Seguridad y Privacidad de la Información, al Programa Integral de Gestión de Datos Personales PIGDP o al Modelo de Seguridad y Privacidad de la Información – MSPI.
- Cuando se materializa un incidente relacionado con el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, al Programa Integral de Gestión de Datos Personales - PIGDP o al Modelo de Seguridad y Privacidad de la Información – MSPI.
- Cuando existan cambios sustanciales en las metodologías que soportan la gestión de riesgos de seguridad de la información y protección de datos personales.
- Cuando se identifica un nuevo activo de información dentro de la entidad o el activo cambie de dueño/responsable/área.

En los proyectos, la gestión de riesgos de seguridad de la información debe tener la misma aplicación metodológica definida por la Oficina de Seguridad de la Información – OSI.

c) Riesgos de Seguridad y Salud en el Trabajo

Para gestionar los riesgos relacionados con Seguridad y Salud en el Trabajo, la entidad se basa en la metodología definida en la Guía GTC-45 Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud

ocupacional, y para los temas relacionados con riesgo sicosocial, atención y prevención de emergencias se utilizarán las metodologías específicas dispuestas por la normatividad colombiana vigente, en el marco de lo establecido en el Sistema de Gestión de la Seguridad y Salud, señalado en el Decreto 1072 de 2015 (Decreto Único Reglamentario del Sector Trabajo).

Nota: Los riesgos asociados a los escenarios de continuidad del negocio están relacionados con los diferentes tipos de riegos institucionales, según aplique.

6.1. NIVEL ACEPTABLE POR TIPO DE RIESGO

El apetito de riesgo o nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, en el marco legal y las disposiciones de la Alta Dirección, se determina en coherencia con las metodologías aplicadas para cada tipo de riesgo.

- **Los riesgos de fraude y corrupción** no son aceptables en la entidad, y su prevención será responsabilidad de todos los servidores públicos de acuerdo con el desarrollo de sus funciones. Los riesgos de fraude y corrupción no podrán ubicarse en las zonas de riesgo aceptable y moderado, y siempre tendrán un plan de acción asociado.

- **Los riesgos estratégicos, operacionales, ambientales y fiscales** se deben gestionar por medio de los controles y dependiendo de su ubicación en la zona de riesgo residual se definen los siguientes tratamientos:

Zona riesgo residual		Decisión tratamiento riesgo residual
	Inaceptable	Se debe reducir, para lo cual se dan dos opciones: • Transferir: tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. • Mitigar: establecer plan de acción.
	Importante	
	Moderado	Se asume el riesgo y se realiza seguimiento a los controles definidos. El responsable del proceso puede realizar un plan de acción si lo considera necesario.
	Aceptable	Se acepta el riesgo y se realiza seguimiento a los controles definidos.

- **Los riesgos de seguridad de la información** los cuales incluyen los riesgos de ciberseguridad y protección de datos personales reconocen los niveles de riesgo aceptable, moderado, importante e inaceptable y establece que únicamente asumirá los riesgos que sean definidos como aceptables.

Para los riesgos que sean identificados como moderados, importantes e inaceptables se deberá ejecutar las acciones necesarias definidas en la metodología de gestión de riesgos de seguridad de la información para mitigarlos.

Los riesgos de seguridad de la información deben llevar a cabo las acciones necesarias para reducir los riesgos a niveles aceptables y se deben agotar los esfuerzos para reducir los impactos y las probabilidades. A su vez, se deben llevar a cabo las actividades para el tratamiento de los riesgos basados en buenas prácticas

- **Los riesgos de capital humano** no podrán ubicarse en zona de riesgo aceptable, y siempre tendrán un plan de tratamiento. Nota: La actitud frente al riesgo puede cambiar a medida que se logre un mayor nivel de madurez en su implementación a nivel institucional.

- **Los riesgos de seguridad y salud en el trabajo** reconocen los niveles de riesgo aceptable, mejorable, aceptable con control específico y no aceptable. Para los riesgos que queden ubicados en zona no aceptable se debe suspender actividades hasta que el riesgo este bajo control y/o realizar una intervención urgente sobre el peligro detectado.

6.2. MONITOREO Y SEGUIMIENTO

Teniendo en cuenta las responsabilidades definidas en el numeral 5. Tabla 2. Responsabilidad y autoridad frente a la gestión de riesgos de este documento, se resalta que, para el monitoreo y seguimiento de la gestión de riesgos institucionales, la entidad se basa en el marco del esquema de líneas de defensas, así:

Primera línea de defensa: el monitoreo de la gestión de riesgos institucionales está bajo la responsabilidad de los líderes de los procesos, quienes periódicamente deben hacer monitoreo a la ejecución de los controles y la efectividad de los mismos, según el proceso que lideren y retroalimentar a los dueños de los macroprocesos.

Así mismo, todos los servidores públicos atendiendo a su nivel jerárquico y al desarrollo de sus funciones, son responsables de la ejecución de los controles y de reportar aquellos eventos que se materialicen, para que los responsables de los procesos establezcan las acciones a que haya lugar de acuerdo con los procedimientos e instrumentos definidos en la entidad para el respectivo reporte y gestión, según el tipo de riesgo.

Segunda línea de defensa: las dependencias responsables de la metodología por cada tipo de riesgo de acuerdo con la **tabla 1. Responsables metodológicos por tipo de riesgo institucional** deben realizar el seguimiento periódico a los riesgos y controles aplicados por la primera línea de defensa, según corresponda, permitiendo que se generen alertas y orientaciones que conlleven al análisis y establecimiento de posibles mejoras por parte de la primera línea de defensa y la línea estratégica.

Para esto, deben elaborar el respectivo informe de seguimiento de acuerdo con el tipo de riesgo del cual es responsable, y enviarlo a la Subdirección de Procesos con la periodicidad que ésta defina para su consolidación y presentación en el Comité Institucional de Coordinación de Control Interno.

Tercera línea de Defensa: la evaluación independiente de la gestión de riesgos institucionales corresponde a la Oficina de Control Interno.

Línea estratégica: en el Comité Institucional de Coordinación de Control Interno se realizará seguimiento a la gestión de riesgos institucionales, teniendo en cuenta el monitoreo y seguimiento realizado por la primera y segunda línea de defensa, y con base a estos informes o seguimientos, así como a la retroalimentación de la tercera línea de defensa; se debe realizar un análisis y en caso de que aplique definir las acciones estratégicas necesarias para enfrentar situaciones críticas que pueden afectar el cumplimiento de los objetivos estratégicos, metas, prestación del servicio y la continuidad del negocio.

6.3. COMUNICACIÓN Y SOCIALIZACIÓN

Una vez aprobada la Política por parte del Comité Institucional de Coordinación de Control Interno, se debe publicar en la DIANNET, así mismo, se debe comunicar y socializar con los servidores públicos de la entidad, con el fin de generar apropiación sobre la gestión del riesgo.

Los responsables de los procesos deben asegurar la divulgación y socialización de sus riesgos.

6.4. GESTIÓN DE LA INFORMACIÓN RELACIONADA CON LA ADMINISTRACIÓN DE RIESGOS DE LA UAE DIAN

La información gestionada dentro de la Administración de Riesgos de la UAE DIAN, se realizará conforme con las disposiciones legales vigentes especialmente lo referente a:

- La información relacionada con el Sistema de Gestión de Riesgos Tributarios, Aduaneros y Cambiarios – Cumplimiento TAC, será tratada conforme con la reserva establecida en el artículo 130 de la Ley 2010 de 2019 “Ley de Crecimiento Económico”: “**Artículo 130. Información del Sistema de Gestión de Riesgos de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales.** La información y procedimientos que administra el sistema de Gestión de Riesgos de la Dirección de Impuestos y Aduanas Nacionales (DIAN) tienen carácter reservado. Esta reserva especial le será oponible a particulares y a todas las entidades públicas, y solo podrá levantarse por orden de autoridad judicial competente.”

- La información relacionada con el Sistema de Gestión de Riesgos Institucionales definidos en la presente política, será tratada conforme con lo dispuesto en la Ley 1712 de 2014 “Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional” y demás disposiciones constitucionales, legales o instancias judiciales que definan situaciones especiales sobre confidencialidad, reserva o clasificación de la información.

7. TÉRMINOS Y DEFINICIONES

- **Activo de información:** elemento de información que se recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes. En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta que tenga valor para la entidad, por ejemplo: archivos, bases de datos, expedientes, entre otros. *Fuente: Superintendencia de Industria y Comercio - Metodología para la Identificación, Clasificación y Valoración de Activos de Información. Hipervínculo: https://sigi.sic.gov.co/SIGI/portal/view_versions.php?&id_doc=1148&version=1&pdf=1*.

- **Administración de riesgos de la UAE DIAN:** comprende la gestión de los riesgos asociados a la implementación, mantenimiento y mejora de los siguientes sistemas:
  Sistema de Gestión de Riesgos Tributarios, Aduaneros y Cambiarios - Cumplimiento TAC.
  Sistema de Gestión de Riesgos Institucionales.
  Fuente: Subdirección de Procesos.

- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública – DAFP.*

- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Causa inmediata**: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Causa raíz**: causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Confidencialidad:** propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información. *Fuente: Instituto Nacional de Ciberseguridad (INCIBE) – España. Hipervínculo: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.*

- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Control:** medida que permite reducir o mitigar un riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. *Fuente: Superintendencia de Industria y Comercio - Metodología para la Identificación, Clasificación y Valoración de Activos de Información. Hipervínculo: https://sigi.sic.gov.co/SIGI/portal/view_versions.php?&id_doc=1148&version=1&pdf=1.*

- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar la organización con relación al riesgo. *Fuente: NTC ISO 31000:2018. Gestión de riesgos.*

- **Impacto**: son las consecuencias a las cuales se ve expuesta la organización en caso de materializarse un riesgo. Como pueden ser la afectación económica (o presupuestal) y reputacional, entre otros. *Fuente: Basado en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Integridad:** propiedad de la información relacionadas con su exactitud y completitud. *Fuente: Superintendencia de Industria y Comercio - Metodología para la Identificación, Clasificación y Valoración de Activos de Información. Hipervínculo: https://sigi.sic.gov.co/SIGI/portal/view_versions.php?&id_doc=1148&version=1&pdf=1.*

- **Línea estratégica de defensa:** está conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno. La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión para toda la entidad. *Fuente: Manual operativo del Modelo Integrado de Planeación y Gestión. Consejo para la gestión y desempeño institucional – Función Pública. V5. 2023.*

- **Primera línea de defensa:** esta línea de defensa les corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad.
  Así mismo, líderes o responsables de procesos que deben aplicar controles de gerencia operativa. Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos. *Fuente: Manual operativo del Modelo Integrado de Planeación y Gestión. Consejo para la gestión y desempeño institucional – Función Pública. V5. 2023.*

- **Segunda línea de defensa:** está conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.
  Permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica).
  Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos. *Fuente: Manual operativo del Modelo Integrado de Planeación y Gestión. Consejo para la gestión y desempeño institucional – Función Pública. V5. 2023.*

- **Tercera línea de defensa:** está conformada por la Oficina de Control Interno, quienes evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos. *Fuente: Manual operativo del Modelo Integrado de Planeación y Gestión. Consejo para la gestión y desempeño institucional – Función Pública. V5. 2023.*

- **Política para la gestión del riesgo**: declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Probabilidad**: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública – DAFP.*

- **Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
  Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgos ambientales:** posibilidad de generar daño en el ambiente, debido tanto a un fenómeno natural como a la acción humana en el desarrollo de las operaciones. *Fuente: Subdirección de Procesos y Riesgos Operacionales.*

- **Riesgo de capital humano:** incapacidad de maximizar la efectividad de la administración tributaria debido a la falta de competencia, capacidad, cumplimiento, costo y compromiso de sus funcionarios. *Fuente: Herramienta de evaluación y diagnóstico de la administración tributaria-TADAT.2019.*

- **Riesgo de corrupción**: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgo de seguridad de la información**: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. *Fuente: Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5. (2020). Hipervínculo:*https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf/50bff85a-70c6-dd15-68f5-6cd2ea2a8707?t=1677003002032

- **Riesgo de Seguridad y Salud en el trabajo:** combinación de la probabilidad de que ocurra una o más exposiciones o eventos peligrosos y la severidad del daño que puede ser causada por éstos. F*uente: Decreto 1072/2015. Art. 2.2.4.6.2 numeral 34.*

- **Riesgos estratégicos:** son aquellos riesgos que pueden afectar el logro, desarrollo y/o ejecución de los objetivos estratégicos o de los elementos estratégicos de la UAE DIAN que hagan sus veces. Se obtienen a partir del ejercicio de análisis y contexto estratégico, el cual hace parte de la formulación del Plan Estratégico cuatrienal. *Fuente: Subdirección de Planeación y Cumplimiento.*

- **Riesgo fiscal:** es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgos operacionales:** efecto que se causa sobre los objetivos del proceso, debido a eventos potenciales. Se consideran riesgos operacionales los riegos operativos y administrativos. *Fuente: Adaptado por la Coordinación de Procesos y Riesgos Operacionales. Basado en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgo Inherente**: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgo Residual**: el resultado de aplicar la efectividad de los controles al riesgo inherente. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Seguridad de la Información**: preservación de la confidencialidad, la integridad y la disponibilidad de la información. *Fuente: ISO 35001:2019 Hipervínculo: https://www.iso.org/obp/ui/es/#iso:std:iso:35001:ed-1:v1:es:term:3.26*

- **Sistema de Gestión de Riesgos Institucionales:** comprende el marco y proceso estructurado para la identificación, análisis, valoración, tratamiento y monitoreo de los riesgos que pueden afectar el cumplimiento de sus objetivos institucionales y la operación de los procesos. *Fuente: Subdirección de Procesos*

- **Sistema de Gestión de Riesgos Tributarios, Aduaneros y Cambiarios - Cumplimiento TAC:** comprende el marco para la gestión de riesgos Tributarios, Aduaneros y Cambiarios - Cumplimiento TAC que contempla su gobernabilidad y política, los métodos o modelos para la identificación de riesgos de cumplimiento, para el análisis, valoración y su priorización, también la definición, administración e implementación de estrategias de tratamientos de riesgos de cumplimiento y la evaluación de los mismos, para finalizar con el diseño y/o desarrollo de mecanismos que permitan el monitoreo y evaluación a la ejecución y resultados de las estrategias de tratamiento implementadas. *Fuente: Subdirección de Análisis de Riesgo y Programas.*

- **Tratamiento:** consiste en seleccionar e implementar opciones para abordar el riesgo. *Fuente: NTC ISO 31000:2018. Gestión de riesgos.*