



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

Versión 4 - 16 de junio de 2026

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.....	3
1. DECLARACIÓN Y COMPROMISO DE LA UAE DIAN FRENTE A LA ADMINISTRACIÓN DE SUS RIESGOS.....	5
2. OBJETIVO	7
3. ALCANCE	7
4. PRINCIPIOS.....	7
5. RESPONSABILIDAD Y AUTORIDAD.....	9
6. METODOLOGÍAS POR TIPO DE RIESGO	16
6.1. NIVEL ACEPTABLE POR TIPO DE RIESGO	21
7. MONITOREO, SEGUIMIENTO Y EVALUACIÓN DEL IMPACTO	25
8. COMUNICACIÓN Y SOCIALIZACIÓN	27
9. GESTIÓN DE LA INFORMACIÓN RELACIONADA CON LA ADMINISTRACIÓN DE RIESGOS DE LA UAE DIAN.....	27
10. TÉRMINOS Y DEFINICIONES	28
11. CONTROL DE CAMBIOS	36

INTRODUCCIÓN

La política para la administración de riesgos de la UAE DIAN establece los lineamientos y disposiciones necesarios para que la entidad gestione de forma efectiva su Sistema Integrado de Gestión de Riesgos y asegure la continuidad del negocio.

La administración de riesgos constituye un elemento fundamental para el cumplimiento de los lineamientos estratégicos de la entidad y se concibe como un marco integral, participativo y dinámico, orientado a garantizar la transparencia, la protección de los recursos del Estado y el fortalecimiento de la confianza pública y la justicia fiscal en todo el territorio nacional. En este sentido, proporciona una base estructurada para la planeación estratégica, contribuye al fortalecimiento de la inteligencia institucional y a la toma de decisiones basada en el análisis de datos y evidencias.

La presente política establece la declaración, los compromisos y los lineamientos integrales para la administración de riesgos en todos los niveles de operación de la entidad, orientados a identificar riesgos y a definir estrategias y acciones oportunas que permitan prevenir su materialización, reducir las vulnerabilidades y mitigar las posibles consecuencias negativas a las que pueda estar expuesta la entidad.

También contempla el alcance, objetivo, los principios, la responsabilidad y autoridad frente a la gestión de riesgos, la metodología y niveles de aceptación de acuerdo con el tipo de riesgo, así como términos y definiciones.

Adicionalmente, incorpora aspectos asociados a la Gestión de la Continuidad del Negocio, como componente fundamental de la gestión integral de riesgos de la entidad, orientada a fortalecer la capacidad institucional para anticipar, responder y recuperarse de eventos disruptivos. Lo anterior, mediante la adopción de estrategias, procedimientos y protocolos que promuevan la resiliencia organizacional, minimicen los impactos sobre la operación y reduzcan los tiempos de interrupción de los procesos críticos y la prestación de los servicios esenciales.

Esta política está elaborada considerando lo definido en el Modelo Integrado de Planeación y Gestión – MIPG, en la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública - DAFP, en las normas NTC-ISO 31000 sobre directrices para la gestión del riesgo y NTC-ISO 22301 sobre sistemas de gestión de continuidad del negocio, de la International Organization for Standardization ISO, en el anexo técnico de los Programas de Transparencia y Ética Pública de la Secretaría de Transparencia, en el Decreto 1122 de 2024 “Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado

por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública” y en concordancia con el Código de Buen Gobierno y la Política de Integridad de la entidad. De igual forma, para la gestión de los riesgos de cumplimiento Tributario, Aduanero y Cambiario – TAC, se toman como referentes las mejores prácticas de organismos internacionales como:

- “Compliance Risk Management: Managing and Improving Tax Compliance” de la Organización para la Cooperación y el Desarrollo Económicos OCDE.
- “Compliance Risk Management In The Digital Era” de la Unión Europea UE.

1. DECLARACIÓN Y COMPROMISO DE LA UAE DIAN FRENTE A LA ADMINISTRACIÓN DE SUS RIESGOS

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

- Riesgos de cumplimiento Tributario, Aduanero y Cambiario TAC.
- Riesgos estratégicos.
- Riesgos operacionales.
- Riesgos de capital humano.
- Riesgos de seguridad y salud en el trabajo.
- Riesgos ambientales.
- Riesgos de seguridad de la información (incluyen riesgos de ciberseguridad y protección de datos personales).
- Riesgos fiscales.
- Riesgos para la integridad.

También se administra el Plan de Continuidad del Negocio con el fin de responder a interrupciones en los procesos críticos, así como reanudar, recuperar y restablecer oportunamente la oferta de productos y servicios de la entidad tras estas eventualidades.

En la entidad se asume de forma sistemática la gestión de los riesgos; para tal fin se parte del análisis del contexto interno y externo, considerando factores económicos, tecnológicos, normativos, sociales e institucionales que pueden incidir en el cumplimiento de los objetivos estratégicos. Este análisis permite anticipar cambios en el entorno, identificar riesgos emergentes y fortalecer la capacidad de respuesta institucional frente a escenarios de incertidumbre. También se establecen controles, estrategias de tratamiento y planes de acción 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 como para el cumplimiento de la misión institucional.

Adicionalmente, la UAE DIAN reconoce que la gestión de los riesgos institucionales guarda una estrecha relación con la Gestión de la Continuidad del Negocio en la medida en que, dentro de las diferentes tipologías de riesgos administradas por la entidad se identifican aquellos que pueden afectar la continuidad de sus procesos, servicios y funciones esenciales. Esta identificación permite establecer escenarios de interrupción, evaluar sus posibles impactos y definir y desarrollar oportunamente estrategias de prevención, respuesta y recuperación, orientadas a fortalecer la resiliencia operativa y asegurar la continuidad del servicio misional. No obstante, dada su naturaleza, los riesgos de cumplimiento no generan escenarios de

interrupción de los procesos críticos de la entidad ni afectan su capacidad para continuar operando, razón por la cual no se considera que incidan directamente en la continuidad del negocio.

Para la efectiva gestión de estos riesgos y de la continuidad del negocio, se asignan los recursos administrativos, económicos, financieros y de capital humano calificado, dispuestos a mitigar los niveles de incertidumbre asociados al cumplimiento de los objetivos estratégicos. Esto contribuye a asegurar la continuidad de la prestación del servicio y de las operaciones, promover el cumplimiento voluntario de las obligaciones tributarias, aduaneras y cambiarias, y afianzar la resiliencia institucional.

El Sistema de Gestión de Riesgos de la UAE DIAN se articula con el Programa de Transparencia y Ética Pública; la entidad gestiona los riesgos para la integridad (conflictos de intereses, soborno, corrupción y fraude) y de Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva (LA/FT/FP), para lo cual contempla la identificación, valoración y monitoreo de estos riesgos; adicionalmente, dispone de canales de denuncia y realiza la gestión de la debida diligencia en el conocimiento de las contrapartes.

De igual forma y en el ámbito de sus competencias, se compromete a:

- Realizar acciones tendientes a proteger la integridad pública.
- Prevenir el lavado de activos, la financiación del terrorismo y la proliferación de armas de destrucción masiva (LA/FT/FP), a fin de evitar impactos directos o indirectos en los procesos y en el cumplimiento de la misión de la Entidad.
- Gestionar las diferentes amenazas que puedan afectar el relacionamiento íntegro con partes interesadas.
- Promover la transparencia y la integridad institucional, fortaleciendo la confianza y el respeto por parte de la ciudadanía.

Adicionalmente, con la gestión de los riesgos de cumplimiento tributario, aduanero y cambiario, la UAE DIAN procura:

- Incrementar los niveles de cumplimiento voluntario por parte de los contribuyentes y usuarios aduaneros y cambiarios con respecto a sus obligaciones.
- Enfocarse en los factores que causan el incumplimiento de las obligaciones TAC y disminuir sus brechas.
- Eliminar la discrecionalidad, respetando el principio de legalidad, e incrementar la transparencia y facilitar la rendición de cuentas.
- Responder de manera efectiva y eficiente a las exigencias y desafíos actuales en materia de cumplimiento tributario, aduanero y cambiario.

Dirección de Gestión Estratégica y de Análisis

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

- Generar balance entre la facilitación y control, para enfocar estrategias de acuerdo con el perfil de cumplimiento del contribuyente y/o usuario aduanero y cambiario.
- Hacer el mejor uso posible de los recursos humanos, tecnológicos y financieros disponibles, enfocándose en prioridades institucionales.

Con el propósito de garantizar la actualización permanente de los elementos que conforman la administración del riesgo, la entidad se compromete a revisarlos de manera periódica cuando así lo requieran los cambios en factores internos o externos.

2. OBJETIVO

Establecer e implementar un enfoque integral de administración de riesgos orientado a prevenir su materialización, mediante la aplicación de controles y acciones que permitan mantener niveles de riesgo aceptables, asegurar el cumplimiento normativo, proteger la integridad pública, garantizar la continuidad del negocio, fortalecer la cultura organizacional y promover la mejora continua y la confianza ciudadana en la Entidad.

3. ALCANCE

La presente política aplica a todos los procesos de la UAE DIAN, incluidas las actividades tercerizadas ejecutadas dentro de estos, los diferentes niveles de operación, la prestación de servicios de la entidad y los proyectos ejecutados por la entidad. Su desarrollo se realizará en observancia de las autoridades y responsabilidades asignadas en las líneas de defensa definidas, asegurando una gestión de riesgos integral, coherente, articulada y alineada con los objetivos estratégicos.

4. PRINCIPIOS

Los principios que establecen las bases sobre las cuales se desarrolla, implementa y mejora el Sistema Integrado de Gestión de Riesgos de la UAE DIAN, se basan en la norma NTC-ISO 31000:2018, los cuales son:

- **Objetividad y no discrecionalidad:** consiste en la toma de decisiones basadas en criterios imparciales, objetivos y predeterminados, al amparo del principio de legalidad, garantizando la equidad, la transparencia y la justicia en todos los ámbitos institucionales.

- **Integralidad:** la administración del riesgo está inmersa en todas las actividades de la Entidad y debe gestionarse de manera articulada con todas las tipologías de riesgos, considerando personas, procesos, tecnología, infraestructura y factores externos.
- **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 la administración de riesgos se adaptan y son proporcionales a los contextos externo e interno de la Entidad relacionados con sus objetivos estratégicos.
- **Inclusiva:** la participación apropiada y oportuna de las partes interesadas permite que se consideren sus conocimientos, 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:** la gestión del riesgo debe basarse en información pertinente, confiable, oportuna y completa para apoyar la toma de decisiones.
- **Capital humano:** promover el desarrollo integral y el bienestar de nuestros servidores públicos, reconociendo su valor estratégico para 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 el aprendizaje y la experiencia.
- **Proporcionalidad:** los controles y tratamientos implementados deben ser proporcionales al nivel de riesgo identificado y al valor, criticidad y sensibilidad de los activos de información.

Además de los anteriores, para la gestión de riesgos de seguridad de la información, se establecen los siguientes principios alineados con la norma NTC-ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información – MSPI de la Entidad y el Sistema de Gestión de Seguridad y Privacidad de la Información SGSPI.

- **Protección de la confidencialidad, integridad y disponibilidad:** la gestión de riesgos debe contribuir a preservar la confidencialidad, integridad y disponibilidad de la información durante todo su ciclo de vida.
- **Responsabilidad compartida:** todos los servidores públicos, contratistas, proveedores y terceros que gestionen información son responsables de identificar, reportar y contribuir al tratamiento de los riesgos asociados a la seguridad de la información.

De igual manera, para la Gestión de la Continuidad del Negocio, la entidad establece los siguientes principios tomando como referencia las normas NTC ISO 22301:2019 Seguridad y resiliencia – Sistema de gestión de continuidad de negocio - Requisitos e ISO 22316:2017 Seguridad y resiliencia – Resiliencia organizacional – Principios y atributos; estos son:

- **Resiliencia:** la gestión de continuidad del negocio busca fortalecer la capacidad institucional para responder, adaptarse y recuperarse oportunamente ante incidentes disruptivos, amenazas emergentes y cambios en el entorno, asegurando la continuidad de las operaciones esenciales.
- **Preparación y capacidad de respuesta ante incidentes:** se establecen protocolos para responder rápida y adecuadamente a incidentes que afecten la operación del negocio, reduciendo tiempos de inactividad y efectos adversos.
- **Recuperación y restablecimiento efectivo:** se definen estrategias y planes para asegurar la recuperación oportuna de procesos críticos con niveles mínimos de servicio aceptables.

5. RESPONSABILIDAD Y AUTORIDAD

En el marco de las funciones establecidas para la entidad mediante el Decreto 1742 de 2020, la Resolución 000070 de 2021, la Resolución 000021 de 2022, Resolución 2 de 2024 y demás reglamentación aplicable vigente o aquella normatividad que los

sustituya o modifique, y en concordancia con lo definido en el Modelo Integrado de Planeación y Gestión – MIPG y en la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública - DAFP vigentes, las responsabilidades y autoridades frente al Sistema Integrado de Gestión de Riesgos se establecen bajo un modelo de líneas de defensa aplicables en todos los niveles de la entidad.

De manera general, el modelo de líneas de defensa establece una estructura de responsabilidades para liderar, implementar, orientar y evaluar la administración de riesgos. La línea estratégica de defensa, conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno, es responsable de definir, aprobar y supervisar las políticas de control interno, gestión del riesgo, seguimiento a la gestión y auditoría interna en la entidad. La primera línea de defensa ésta conformada por líderes de procesos, servidores públicos y responsables de proyectos, quienes ejecutan y supervisan las actividades diarias, aplican controles operativos y administran los riesgos mediante su identificación, evaluación, control y mitigación. La segunda línea está conformada por directivos o asesores que supervisan la gestión institucional, realizan seguimiento y autoevaluación permanente, orientan a la primera línea de defensa y verifican la efectividad de los controles y de la gestión de riesgos, generando alertas y promoviendo mejoras con enfoque basado en riesgos. Y la tercera línea corresponde a control interno o auditoría interna, encargada de evaluar de manera independiente la efectividad de la gestión de riesgos.

Para el caso en concreto de la UAE DIAN, la administración de riesgos es coordinada por la Dirección de Gestión Estratégica y de Analítica o quien haga sus veces, junto con los responsables metodológicos por tipo de riesgo, los líderes de los procesos y sus equipos de trabajo.

Los responsables metodológicos por cada tipo de riesgo y de la continuidad del negocio son las siguientes dependencias:

Tabla 1. Responsables metodológicos por tipo de riesgo

Tipo de riesgo	Responsable
Riesgos estratégicos	Subdirección de Planeación y Cumplimiento
Riesgos operacionales, ambientales, de integridad y riesgos fiscales	Subdirección de Procesos Riesgos para la integridad relacionados con LA/FT/FP: Subdirección de Apoyo

Tipo de riesgo	Responsable
	en la Lucha contra el Delito Aduanero y Fiscal (apoyo técnico).
Riesgos de seguridad de la información	Oficina de Seguridad de la Información
Riesgos de Capital humano	Subdirección de Gestión del Empleo Público Subdirección de Desarrollo del Talento Humano Subdirección Escuela de Impuestos y Aduanas
Riesgos de seguridad y salud en el trabajo	Subdirección de Desarrollo de Talento Humano
Riesgos de Cumplimiento TAC	Subdirección de Análisis de Riesgo y Programas

Ahora bien, en los aspectos relacionados con continuidad del negocio, son responsables metodológicos, los siguientes:

- Plan de continuidad del negocio: Subdirección de Procesos.
- Plan de recuperación de desastres tecnológicos DRP: Subdirección de Infraestructura Tecnológica y de Operaciones y Oficina de Seguridad de la Información.
- Planes de emergencia: Dirección de Gestión Corporativa.

A continuación, se establecen los niveles de responsabilidad y autoridad frente a la administración de riesgos y continuidad del negocio aplicables en la entidad, acorde con el modelo de líneas de defensa:

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	En el marco del Comité Institucional de Gestión y Desempeño : • Definir lineamientos estratégicos para la administración del Sistema Integrado de Gestión de Riesgos de la UAE DIAN, asegurar su implementación, seguimiento y mejora continua; así como, gestionar los recursos requeridos para su

Dirección de Gestión Estratégica y de Análítica

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

Línea de defensa	Responsable	Responsabilidad e instancia o nivel
	Institucional de Coordinación de Control Interno Comité Institucional Estratégico o las instancias que hagan sus veces	funcionamiento, incluyendo los instrumentos de protección financiera. - Aprobar los riesgos que se encuentren fuera del apetito de riesgos, previo análisis, según aplique, por los tipos de riesgos. - Seleccionar los riesgos de cumplimiento TAC objeto de análisis, aprobar la priorización de los riesgos y la estrategia de asignación de tratamientos. - A partir de los monitoreos y seguimientos realizados por las demás líneas de defensa, realizar un análisis y tomar las decisiones 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 de Coordinación de Control Interno: - Definir y aprobar la Política para la administración de riesgos, la cual se debe revisar considerando el análisis del entorno, alcance y objetivos que puedan generar cambios en la misma; adicionalmente, debe facilitar su despliegue y entendimiento en todos los niveles de la Entidad. En el marco del Comité Institucional Estratégico: - Analizar y aprobar los protocolos de la Entidad para el manejo de crisis y emergencias.
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 Integrado de Gestión de Riesgos, trabajando en colaboración con las demás líneas de defensa para gestionar adecuadamente los riesgos. - Gestionar cada tipo de riesgo y su actualización, en caso de que se requiera, de acuerdo con las metodologías establecidas en las etapas que les corresponda. - Definir y estructurar los planes de mejora de cumplimiento PMC (aplica solo para los riesgos de cumplimiento). - Realizar monitoreo permanente a la ejecución de los controles y estrategias de tratamiento y evaluar su pertinencia y efectividad. - 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 riesgos de acuerdo con la periodicidad e instancias definidas según el tipo de riesgo e informar lo pertinente 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

1ª línea de defensa

Línea de defensa	Responsable	Responsabilidad e instancia o nivel
		acorde con 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.
2ª línea de defensa	Responsables metodológicos por tipo de riesgo (ver Tabla 1)	- Orientar y acompañar a la primera línea de defensa en la gestión de los diferentes tipos de riesgos de acuerdo con las metodologías establecidas, en las etapas que les correspondan y en la gestión de continuidad del negocio, lo cual incluye la definición de la metodología a utilizar, su revisión, actualización y desarrollo, conforme con las guías, normas y demás documentos aplicables en la entidad y al tipo de riesgo. - Coordinar con la primera línea de defensa la actualización de los riesgos, definiendo y asignando los responsables de participar en esta actividad. Las dependencias metodológicamente responsables por cada tipo de riesgo son las siguientes: 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. Subdirección Escuela de Impuestos y Aduanas: 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 con respecto a los riesgos operacionales, ambientales y riesgos para la integridad, con el apoyo técnico de la Subdirección de Apoyo en la Lucha contra el Delito Aduanero y Fiscal para los riesgos para la integridad relacionados con LA/FT/FP, También es responsable de la orientación frente a los riesgos que afecten la continuidad del negocio con el apoyo de la Subdirección de Infraestructura Tecnológica y de Operaciones y Oficina de Seguridad de la Información para Continuidad TI. Coordina la elaboración del Plan de Continuidad del Negocio con base en los insumos proporcionados por la Subdirección de Infraestructura Tecnológica y de Operaciones, Oficina de Seguridad de la Información y la Dirección de Gestión Corporativa. Subdirección de Infraestructura Tecnológica y de Operaciones, Oficina de Seguridad de la Información: es responsable de la orientación frente a Continuidad Tecnología de la Información - TI y definición del Plan de Recuperación de Desastres Tecnológicos DRP.

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

Línea de defensa	Responsable	Responsabilidad e instancia o nivel
		- Subdirección de Planeación y Cumplimiento: es responsable de la orientación frente a los riesgos estratégicos. - Subdirección de Análisis de Riesgo y Programas o quien haga sus veces: es responsable de definir los lineamientos en materia de riesgos de cumplimiento TAC y realizar acompañamiento metodológico. • Realizar y/o apoyar actividades para fortalecer el entendimiento de la administración de riesgos, tales como sensibilizaciones, capacitaciones, entre otros, según corresponda. • Realizar seguimiento periódico a los riesgos, controles, estrategias de tratamiento y planes de acción implementados 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 toma de decisiones por parte de la línea estratégica. • Implementar actividades de control específicas que permitan realizar 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, la evaluación y monitoreo al cumplimiento normativo, entre otros.
2ª línea de defensa	Función de Cumplimiento	Quien asuma la Función de Cumplimiento es responsable de: • Velar por la efectiva, eficiente y oportuna gestión de riesgos para la integridad, apoyando a los líderes de procesos y gestores de riesgo en dicha responsabilidad. • Evaluar la gestión de riesgos para la integridad y presentar, en la periodicidad que se establezca, los resultados de la evaluación a la Alta Dirección. Estas evaluaciones deberán contemplar: - Resultados de la gestión desarrollada en el marco de la función de cumplimiento. - Reportes de operaciones generados en el marco de la gestión del riesgo. - Planes de mejoramiento asociados a la gestión de riesgos para la integridad implementados, en el marco del proceso de mejora continua. • Revisar y recomendar la implementación de los lineamientos que el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República, la Unidad de Información y Análisis Financiero, y las entidades de control, expidan en temas relacionados con la gestión del riesgo. • Articular con las dependencias competentes las acciones necesarias para garantizar la operatividad de la gestión de riesgos para la integridad, así como promover el desarrollo de

Línea de defensa	Responsable	Responsabilidad e instancia o nivel
		programas internos de capacitación orientados al cumplimiento y fortalecimiento de esta gestión. • Colaborar con el diseño de las metodologías, modelos e indicadores que requiera la gestión de riesgos para la integridad, con la actualización de los elementos existentes, y la promoción de medidas correctivas necesarias, velando por su implementación y comunicación oportuna a todas las partes interesadas. • Establecer los lineamientos institucionales para la aplicación proporcional basada en riesgos, de los mecanismos de debida diligencia en el conocimiento de las contrapartes. • Elaborar y someter a aprobación de la Alta Dirección, los criterios objetivos para la determinación de las operaciones inusuales y sospechosas. • Reportar a la Unidad de Información y Análisis Financiero - UIAF, las operaciones inusuales o sospechosas que se hayan identificado conforme con los criterios definidos y el procedimiento institucional adoptado. • Reportar a la Fiscalía General de la Nación o a la autoridad que corresponda, posibles comportamientos anómalos que se identifiquen en la entidad y puedan considerarse posible delito.
3ª línea de defensa	Oficina de Control Interno	• Realizar la evaluación (aseguramiento) independiente sobre la gestión de los riesgos según aplique. Informar los hallazgos y riesgos materializados y proporcionar recomendaciones a las demás líneas de defensa. • Evaluar y verificar que la gestión de riesgos se desarrolla de acuerdo con los lineamientos, políticas y procedimientos definidos para la Entidad. • Evaluar la efectividad de los controles para evitar la materialización de riesgos. • Apoyar y asesorar en la gestión de riesgos según se requiera. • Evaluar que el Plan de Continuidad de Negocio (PCN) de la entidad esté correctamente diseñado, implementado y mantenido, con el fin de que los procesos críticos puedan seguir funcionando ante emergencias o desastres, conforme a los lineamientos institucionales.

6. METODOLOGÍAS POR TIPO DE RIESGO

En el marco del Modelo Integrado de Planeación y Gestión (MIPG) y en concordancia con la norma NTC-ISO 31000:2018, que establece directrices para la gestión del riesgo, la entidad ha definido que, para la gestión de los diferentes tipos de riesgos, así como para la definición e implementación de controles, estrategias de tratamiento y planes de acción, se deberán considerar las siguientes disposiciones:

Dirección de Gestión Estratégica y de Análítica

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

Para la identificación de los riesgos, es necesario realizar un análisis integral del entorno en el que opera la entidad, tanto a nivel interno como externo. Esto permite comprender su realidad institucional y su interacción con el entorno, incluidos los contribuyentes y los usuarios aduaneros y cambiarios, facilitando la identificación de factores que podrían afectar el desarrollo de los procesos, el cumplimiento de los objetivos misionales, así como la transparencia y la ética institucional.

En el marco de la Dimensión 2: Direccionamiento Estratégico del MIPG, la gestión de riesgos en la UAE DIAN se articula de manera directa con la planeación estratégica institucional. En este sentido, los riesgos se identifican, analizan y gestionan en función de su impacto sobre el cumplimiento de los objetivos, planes, programas y proyectos de la entidad, lo cual permite orientar la toma de decisiones, priorizar acciones y fortalecer el logro de los resultados institucionales.

A partir de los riesgos identificados en cada proceso, se establecerán aquellos que puedan afectar la continuidad del negocio. Estos riesgos deberán contar dentro de sus tratamientos, con controles orientados al desarrollo de estrategias de recuperación o restablecimiento del servicio. En consecuencia, el Plan de Continuidad de Negocio toma como insumo la identificación de los riesgos que puedan generar interrupciones en los procesos críticos de la entidad o en los recursos necesarios para su ejecución, conforme con lo determinado en el Análisis de Impacto del Negocio (BIA). Con base en ello, se definirán los escenarios de no continuidad y las estrategias de recuperación requeridas para garantizar la continuidad operativa. Este análisis se realizará teniendo en cuenta los lineamientos definidos por la entidad en la cartilla CT-PEC-0156 Metodología Plan de Continuidad del Negocio - PCN, los cuales se basan principalmente en elementos de la norma NTC ISO 22301:2019 Seguridad y resiliencia - Sistema de gestión de continuidad de negocio y las mejores prácticas internacionales en Gestión de la Continuidad, dando cumplimiento a los lineamientos del Ministerio de Tecnologías de la Información y las comunicaciones – MINTIC en el marco de las políticas de Gobierno Digital y Seguridad Digital.

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

a) Riesgos estratégicos, operacionales, ambientales, fiscales, de integridad y capital humano

La metodología para administrar los riesgos estratégicos, operacionales, ambientales, fiscales, de integridad y de capital humano se basa en los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública - DAFP; y en la norma NTC ISO 14001:2015 Sistemas de Gestión Ambiental para los riesgos ambientales, así como en los lineamientos de la Secretaría de Transparencia de la Presidencia de la República para el caso de los riesgos para la integridad, 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.

Adicionalmente, la entidad cuenta con documentos de apoyo para gestionar los riesgos para la integridad, los cuales son:

- **Gestión de la debida diligencia en el conocimiento de las contrapartes:** En desarrollo de la debida diligencia en todas las interacciones con las contrapartes, en las que exista una exposición a riesgos para la integridad pública, es una medida preventiva el adecuado conocimiento de las contrapartes: Para este fin, la UAE DIAN cuenta principalmente con los siguientes documentos:
 - MN-ADF-0013 Manual de Contratación
 - CT-ADF-0109 – Cartilla de supervisión y/o interventoría
 - Procedimientos para las etapas contractuales (PR-ADF-0433 Etapa contractual, PR-ADF-0434 Etapa poscontractual y PR-ADF-0435 Etapa precontractual)
 - PR-TAH-0061 Procedimiento Vinculación de Personal

La entidad tiene la obligación de mantener los documentos y registros de las contrapartes y sus operaciones por el término dispuesto en el artículo 12 de la Ley 2195 de 2022, asegurando la confidencialidad de la información clasificada y reservada, el correcto tratamiento de los datos personales, su archivo y custodia.

- **Herramientas de gestión de riesgos para la integridad:** la entidad cuenta con políticas, procedimientos y demás documentos que sirven para guiar la conducta de los servidores públicos, fomentando una cultura de ética, transparencia y responsabilidad.
 - CG-PEC-0001 Código de buen gobierno.

Dirección de Gestión Estratégica y de Análisis

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

- CG-TAH-0002 Código de Integridad.
- CT-TAH-0128 Guía para la gestión y trámite del conflicto de intereses en la entidad.
- **Operación del canal institucional de denuncias por corrupción:** la entidad cuenta con procedimientos que establecen los pasos a seguir para recibir, evaluar y tramitar las denuncias, incluidas aquellas asociadas a integridad:
 - PR-CAC-0043 Peticiones, quejas, sugerencias, reclamos, felicitaciones y denuncias.
 - PR-CAC-0450 Trámite a denuncias enviadas a la dirección general.
 - PR-COT-0375/ PR-COA-0375 Gestión denuncias de fiscalización.
 - PR-TAH--0478 Instrucción disciplinaria instrucción disciplinaria.
 - PR-PEC-0120 Atención a procesos penales.
- **Operación del canal institucional para el Reporte de Operaciones Sospechosas – (ROS):** la entidad cuenta con procedimientos que establecen los pasos a seguir para recibir, evaluar y tramitar los reportes de operación sospechosa asociados con LA/FT/FP ante la UIAF:
 - PR-COT-0316/PR-COA-0316 Gestión de reportes de operación sospechosa de LA/FT.
- **Función de cumplimiento:** El Director General de la UAE DIAN definirá el rol que representará la función de cumplimiento en la entidad y cuyas responsabilidades se encuentran en el capítulo 5. Responsabilidad y Autoridad. Tabla 2 Responsabilidad y autoridad frente a la gestión de riesgos del presente documento.

b) Riesgos de seguridad de la Información

La metodología para la gestión de riesgos de seguridad de la Información está basada en los lineamientos establecidos en la versión vigente de la Guía para la Gestión Integral del Riesgo en Entidades Públicas Departamento Administrativo de la Función Pública - DAFP y los lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (versión vigente) del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC.

Esta metodología determina que, cuando se cumpla al menos uno de los siguientes criterios, es necesario iniciar una evaluación de riesgos de seguridad de la información en la entidad, así:

- Activos con Disponibilidad “Alta”: aquellos cuya valoración final en la dimensión de “Disponibilidad” sea clasificada como “ALTA”.
- Activos con valoración “Alta”: aquellos cuya valoración consolidada (considerando Confidencialidad, Integridad y Disponibilidad) sea clasificada como “ALTA”.
- Activos con Datos Personales: únicamente aquellos que contengan datos personales sensibles, semiprivados o privados al momento de su identificación.
- Activos relacionados con Autenticación Digital: activos de tipo software que requieran autenticación digital para su acceso y uso.
- Cuando se determine que el activo soporta la Infraestructura Crítica Cibernética (ICC) de la DIAN.

La metodología para la gestión de activos y riesgos de seguridad de la información está establecida en la cartilla CT-IIT-0132 Gestión de Riesgos de Seguridad de la Información y en la cartilla para la gestión de activos de información CT-IIT-0079.

En los proyectos tecnológicos, 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 psicosocial, 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).

d) Riesgos de cumplimiento TAC

La metodología para la gestión de riesgos de cumplimiento TAC se basa en las mejores prácticas internacionales, principalmente el modelo de gestión de riesgos definido por la Organización para la Cooperación y el Desarrollo Económico – OCDE, el cual se representa en la gráfica 1.

Gráfica 1. Modelo gestión de riesgos OCDE



Fuente: Centro Interamericano de Administraciones Tributarias – CIAT. 2020.

Este modelo se fundamenta en el análisis del comportamiento de los contribuyentes, así como de los usuarios aduaneros y cambiarios, respecto al cumplimiento de sus obligaciones. A partir de la identificación de las causas que determinan dicho comportamiento, se orienta al diseño de estrategias de tratamiento que promuevan y fortalezcan el cumplimiento voluntario.

Al igual que el análisis del comportamiento de los contribuyentes, es importante analizar diversa información (cuantitativa y/o cualitativa) y realizar las combinaciones posibles para determinar indicadores de riesgo global o específico o transaccional.

Los riesgos de cumplimiento TAC deben priorizarse mediante un proceso de jerarquización y consolidación, con el fin de identificar aquellos que serán objeto de la aplicación de estrategias de tratamiento.

6.1. NIVEL ACEPTABLE POR TIPO DE RIESGO

La UAE DIAN define su apetito de riesgo como el nivel de riesgo que está dispuesta a aceptar en el desarrollo de sus actividades, con el fin de lograr sus objetivos en el marco del cumplimiento normativo, la protección de los recursos públicos y la generación de valor público.

En este sentido, el apetito de riesgo orienta la toma de decisiones estratégicas y operativas, permitiendo establecer criterios frente a los riesgos que pueden ser asumidos, mitigados, transferidos o evitados.

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 estratégicos, operacionales, ambientales, de capital humano, fiscales y de integridad** se deben gestionar por medio de los controles, y, según su ubicación en la zona de riesgo residual, se definen los siguientes tratamientos:

Tabla 3. Decisión del tratamiento para el riesgo residual, según tipo de riesgo

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	Opciones: • Transferir: tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. • Se realiza seguimiento a los controles definidos. El responsable del proceso puede realizar un plan de acción si lo considera necesario o si existen iniciativas al interior del proceso que contribuyan a gestionar los riesgos.
	Moderado	Se realiza seguimiento a los controles definidos. El responsable del proceso puede realizar un plan de acción si lo considera necesario o si existen iniciativas al interior del proceso que contribuyan a gestionar los riesgos.
	Aceptable	Se acepta el riesgo y se realiza seguimiento a los controles definidos.

Los riesgos para la integridad como el soborno, fraude, corrupción, conflicto de intereses y lavado de activos, financiación del terrorismo y financiación para la proliferación de armas de destrucción masiva – LA/FT/FP no son aceptables y su prevención será responsabilidad de todos los servidores públicos de acuerdo con el desarrollo de sus funciones.

Además, es necesario gestionar los conflictos de interés de conformidad con los lineamientos definidos en la Entidad, particularmente los establecidos en la cartilla CT-TAH-0128 Guía para la gestión del conflicto de intereses en la Entidad.

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

Para los riesgos que sean identificados como moderados, importantes e inaceptables, se deberán 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 gestionarse mediante la implementación de controles y acciones orientadas a su mitigación, con el fin de reducirlos a niveles aceptables. Para ello, se deben definir e implementar medidas que permitan disminuir su probabilidad de ocurrencia e impacto asociado. Así mismo, es indispensable ejecutar las actividades de tratamiento de riesgos conforme con buenas prácticas.

- **Para los riesgos de seguridad y salud en el trabajo** se 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 deben suspender actividades hasta que el riesgo este bajo control y/o realizar una intervención urgente sobre el peligro detectado.
- **Para los riesgos de cumplimiento TAC** se reconocen los siguientes niveles de riesgo:

Tabla 4. Descripción de los niveles de riesgo

Nivel de riesgo	Descripción
Bajo	Corresponde a consecuencias bajas y probabilidad de ocurrencia rara o improbable.
Moderado	Corresponde a consecuencias bajas y probabilidad de ocurrencia moderada o probable, o bien, consecuencias medias y probabilidad de ocurrencia rara o improbable.
Significativo	Corresponde a consecuencias bajas y probabilidad de ocurrencia muy probable, o bien, consecuencias medias y probabilidad de ocurrencia moderada, probable o muy probable, o bien, consecuencias altas y probabilidad de ocurrencia rara.
Alto	Corresponde a consecuencias altas y probabilidad de ocurrencia improbable, moderada, probable o muy probable, o bien, consecuencias muy altas y probabilidad de ocurrencia

Nivel de riesgo	Descripción
	rara, improbable o moderada; o bien consecuencias extremas y probabilidad de ocurrencia rara o improbable.
Severo	Corresponde a consecuencias muy altas y probabilidad de ocurrencia probable o muy probable, o bien, consecuencias extremas y probabilidad de ocurrencia moderada, probable o muy probable.

Decisión del tratamiento de los riesgos de cumplimiento TAC:

Los tratamientos a aplicar se definirán en estrategias institucionales basadas en efectividad histórica, capacidad operativa, prioridades estratégicas, análisis de datos e integración de riesgos. Los tratamientos se pueden implementar de acuerdo con la disposición al cumplimiento por parte de los contribuyentes, usuarios aduaneros y cambiarios, como se muestra en la siguiente gráfica:

Gráfica 2. Estrategias a aplicar según la disposición al cumplimiento por parte de los contribuyentes, usuarios aduaneros y cambiarios



Fuente: Subdirección de Análisis de Riesgo y Programas a partir del modelo experiencia DIAN y del modelo de la Estrategia del Cumplimiento – FMI.

- **Continuidad de negocio:** se definen los siguientes niveles para la Continuidad del negocio.

Tabla 5. Descripción de los niveles de impacto para continuidad del negocio

Nivel de impacto	Descripción	Tratamiento
Crítico	Nivel intolerable. Parálisis total o prolongada de trámites o servicios de cara al contribuyente o usuario aduanero o cambiario.	Estrategias definidas en PCN y gestión y manejo de crisis por parte del PMU
Grave	Detiene parcialmente trámites o servicios de cara al contribuyente o usuario aduanero o cambiario.	Estrategias definidas en PCN y gestión por parte de la mesa de incidentes.
Moderado	Interrupciones menores y temporales que no afectan significativamente la prestación de servicios o trámites de cara al contribuyente o usuario aduanero o cambiario que pueden resolverse	Recuperación del servicio y monitoreo por parte del responsable del proceso afectado

7. MONITOREO, SEGUIMIENTO Y EVALUACIÓN DEL IMPACTO

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, seguimiento y evaluación de impacto, la entidad se basa en el marco del esquema de líneas de defensa, así:

- **Línea estratégica:** en el Comité Institucional de Gestión y Desempeño se realizará seguimiento a la administración de riesgos de la entidad, teniendo en cuenta el monitoreo, seguimiento y evaluación de impacto (la evaluación de impacto aplica para los riesgos de cumplimiento TAC) realizado por la primera y segunda línea de defensa, así como los informes 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.
- **Primera línea de defensa:** el monitoreo de la gestión de riesgos está bajo la responsabilidad de los líderes de los procesos, quienes periódicamente deben

Dirección de Gestión Estratégica y de Análítica

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

hacer seguimiento a la ejecución de los controles y estrategias de tratamiento y a la efectividad de estos, según el proceso que lideren e informar lo pertinente a los dueños de los macroprocesos.

En este sentido, todos los servidores públicos atendiendo a su nivel jerárquico y en desarrollo de sus funciones, son responsables de la ejecución de los controles e implementación de las estrategias de tratamiento, así como 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.

Para los riesgos de cumplimiento TAC, la Dirección de Gestión de Fiscalización, Dirección de Gestión de Aduanas, Dirección de Gestión de Impuestos y Dirección Operativa de Grandes Contribuyentes, así como las Direcciones Seccionales son responsables de realizar el monitoreo y reporte de los resultados alcanzados en la implementación de controles y estrategias de tratamiento.

En cuanto a la continuidad de negocio, cuando se presenten incidentes que afecten la continuidad del negocio, la mesa de incidentes o el PMU realizarán el balance post-incidente o post-crisis respectivamente, una vez declarado el cierre del incidente, de conformidad con los protocolos OD-PEC-0003 Manejo de incidentes e identificación de crisis y OD-PEC-0004 Manejo de Crisis.

- **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”, deben realizar el seguimiento periódico a los riesgos, controles y estrategias de tratamiento 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 toma de decisiones por parte de la línea estratégica.

Para esto, deben elaborar el respectivo informe de seguimiento de acuerdo con el tipo de riesgo del cual es responsable, para su presentación en el Comité Institucional de Gestión y Desempeño o quien haga sus veces.

Quien asuma el rol de **Función de Cumplimiento** en la Entidad debe evaluar la gestión de riesgos para la integridad y presentar a la Alta Dirección, en la periodicidad que se establezca, los resultados de la evaluación y los planes de mejoramiento asociados a la gestión de estos riesgos, en el marco del proceso de mejora continua.

Para la gestión de continuidad de negocio, se implementará un programa anual de ejercicios y pruebas para evaluar la capacidad institucional de respuesta ante interrupciones y validar a lo largo del tiempo la efectividad de los protocolos para el manejo de incidentes y crisis, así como de las estrategias de tratamiento y planes de recuperación definidos.

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

8. COMUNICACIÓN Y SOCIALIZACIÓN

Una vez aprobada la Política por parte del Comité Institucional de Coordinación de Control Interno, deberá publicarse en cumplimiento de las disposiciones vigentes en materia de publicidad y transparencia. Adicionalmente, deberá ser comunicada y socializada entre los servidores públicos de la entidad, con el fin de promover su apropiación y fortalecer la administración del riesgo.

Los responsables de los procesos deben asegurar la divulgación y socialización de sus riesgos y del Plan de Continuidad de Negocio, según aplique.

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

La gestión de la información atinente a la administración de riesgos de la UAE DIAN, se realizará acatando las disposiciones legales vigentes, especialmente las siguientes:

- La información relacionada con la gestión de Riesgos de Cumplimiento, Tributarios, Aduaneros y Cambiarios 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.”.

No obstante, con respecto a la no oponibilidad de reserva a la Contraloría General de la República, se debe tener en cuenta lo establecido en el artículo 1 del Acto Legislativo 04 de 2019, por medio del cual se reforma el régimen de control fiscal.

- La información relacionada con los demás riesgos referidos en esta 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.

10. 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, transmitida 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 administración del sistema de gestión de los riesgos de la entidad, cuyas etapas están asociadas a su planificación, implementación, mantenimiento y mejora. *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 Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública – DAFP.*
- **BIA - Análisis de impacto de negocio:** proceso en el que se analiza el impacto de una interrupción conforme avanza el tiempo, en la organización. *Fuente: Norma NTC ISO 22301:2019 Seguridad y resiliencia. Sistema de Gestión de Continuidad de Negocio. ICONTEC.*
- **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: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. 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: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. 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/quia_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: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Continuidad del negocio:** capacidad de la organización para continuar con la oferta de productos y servicios dentro de un período de tiempo aceptable a una capacidad predefinida durante una interrupción. *Fuente: Norma NTC ISO 22301:2019 Seguridad y resiliencia. Sistema de Gestión de Continuidad de Negocio. ICONTEC.*
- **Contraparte:** cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Control:** medida que permite reducir o mitigar un riesgo. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Debida diligencia:** proceso que deben llevar a cabo las entidades para identificar, prevenir, mitigar y explicar cómo abordan los impactos negativos reales y potenciales en sus propias actividades, su cadena de suministro y otras relaciones comerciales. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Debida diligencia en el conocimiento de la contraparte:** proceso que le permite a la entidad conocer aspectos relevantes de sus contrapartes, sean partes vinculadas o relacionadas, para poder gestionar el riesgo que cualquier vinculación o relacionamiento genera. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. 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://siji.sic.gov.co/SIGI/portal/view_versions.php?&id_doc=1148&version=1&pdf=1.

- **Función de cumplimiento:** función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **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 Gestión Integral del Riesgo en Entidades Públicas V7, 2025. 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://siji.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. V6. 2024.*
- **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. V6. 2024.*

- **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. V6. 2024.*

- **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; además, 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. V6. 2024.*
- **Mesa de incidentes:** instancia de coordinación donde se analiza el incidente y se toman decisiones para su atención inmediata. Puede realizarse por medios digitales o presenciales. Es liderada por el Director Seccional, Director de Gestión, Jefe de Oficina o Director Operativo, según corresponda. *Fuente: UAE DIAN Subdirección de Procesos y Oficina de Seguridad de la Información.*
- **Plan de continuidad del negocio:** información documentada que orienta a una organización para responder a una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad de negocio. *Fuente: Norma NTC ISO 22301:2019 Seguridad y resiliencia. Sistema de Gestión de Continuidad de Negocio. ICONTEC*
- **PMU Puesto de Mando Unificado:** equipo de trabajo convocado por el Director General para gestionar la atención de una crisis con un nivel de impacto crítico, o que requiere de la gobernabilidad de la Dirección General. Puede realizarse por medios digitales o presenciales. *Fuente: UAE DIAN Subdirección de Procesos y Oficina de Seguridad de la Información.*

- **Política de administración de riesgos:** 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: Basado en la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Reporte de Operación Sospechosa:** es aquella operación que por su número, cantidad o características no se enmarca dentro del sistema y prácticas normales del negocio, de una industria o de un sector determinado y, además que de acuerdo con los usos y costumbres de la actividad que se trate, no ha podido ser razonablemente justificada. *Fuente: Unidad de Información y Análisis Financiero – UIAF - Colombia. Hipervínculo: [Reporte de Operación Sospechosa \(ROS\) | UNIDAD DE INFORMACIÓN Y ANÁLISIS FINANCIERO](#)*
- **Resiliencia organizacional:** capacidad de una organización para absorber y adaptarse en un entorno cambiante. *Fuente: Norma ISO 22316:2017 Seguridad y resiliencia - Resiliencia organizacional - Principios y atributos. Hipervínculo: [ISO 22316:2017\(en\). Security and resilience — Organizational resilience — Principles and attributes](#)*
- **Responsables metodológicos:** dependencias asociadas a la segunda línea que participan en la definición de la metodología de riesgos, así mismo, ofrecen orientación y asesoramiento sobre diferentes aspectos metodológicos asociados a su gestión. *Fuente: Subdirección de Procesos.*
- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. 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: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Riesgo ambiental:** 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.*
- **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 cumplimiento TAC:** efecto sobre la incertidumbre en el cumplimiento de las obligaciones tributarias, aduaneras y cambiarias por parte de los contribuyentes y usuarios aduaneros y cambiarios. Estos riesgos están asociados a las dimensiones de cumplimiento registrar, informar, declarar y pagar. *Fuente: Subdirección de Análisis de Riesgo y Programas.*
- **Riesgo de integridad:** toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*

Hay varias amenazas que pueden incidir en diferentes etapas de los procesos organizacionales que terminan afectando la capacidad de una entidad para alcanzar sus objetivos, en particular, asegurar el cumplimiento de la ley. Entre las amenazas asociadas a integridad pública, se encuentran:

- **Conflicto de interés:** se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011). *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Soborno:** ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar.
 - o Soborno entrante: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad.
 - o Soborno saliente: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre

de la entidad. Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.

- **Corrupción:** todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles que atenten contra la administración pública descritas en el Título XV de la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015). Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública – DAFP.
- **Fraude:** errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.
- **Lavado de activos financiación del terrorismo y financiación para la proliferación de armas de destrucción masiva – (LA/FT/FP):** se entiende como la posibilidad de que una entidad sea utilizada para dar apariencia de legalidad a recursos de origen ilícito o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser objeto de cuestionamiento. Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública – DAFP.
- **Lavado de activos (LA):** conducta penal consistente en adquirir, resguardar, invertir, transportar, transformar, almacenar, conservar, custodiar o administrar bienes que provienen de actividades ilícitas como el tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, financiación del terrorismo, tráfico de drogas, contrabando, delitos contra el sistema financiero y la administración pública, entre otros, con el fin de ocultar su origen ilícito o darles apariencia de legalidad a dichos bienes. Fuente: Artículo 323 del Código Penal Colombiano. Ley 599 de 2000.

- **Financiación del Terrorismo (FT):** delito que consiste en proveer, recolectar, entregar, recibir, administrar, aportar, custodiar o guardar fondos, bienes o recursos, directa o indirectamente, o realizar cualquier acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos armados al margen de la ley, grupos de delincuencia organizada, grupos terroristas nacionales o extranjeros, o a sus integrantes, así como a actividades terroristas. *Fuente: Artículo 345 del Código Penal Colombiano. Ley 599 de 2000.*
- **Financiación de la Proliferación de Armas de Destrucción Masiva (FP):** el acto de proveer fondos, servicios financieros u otros activos a disposición, directa o indirectamente, de o para el beneficio de, alguna persona o entidad designada por o bajo la autoridad del Consejo de Seguridad de las Naciones Unidas dentro del Capítulo VII de la Carta de las Naciones Unidas, en lo relativo a la prevención, represión e interrupción de la proliferación de armas de destrucción masiva y su financiamiento. La Financiación de la Proliferación puede darse por: recaudación, transmisión, utilización. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Riesgo de seguridad de la información:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **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. *Fuente: Decreto 1072/2015. Art. 2.2.4.6.2 numeral 34.*
- **Riesgo estratégico:** posibilidad de ocurrencia de eventos internos o externos que pueden afectar el cumplimiento de los lineamientos y objetivos estratégicos de la entidad, incidiendo sobre las capacidades institucionales y el nivel de confianza y calidad en el relacionamiento con nuestros grupos de valor e interés. *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: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgo operacional:** efecto que se causa sobre los objetivos del proceso, debido a eventos potenciales. *Fuente: Subdirección de Procesos UAE DIAN.*
- **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: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. Departamento Administrativo de la Función Pública - DAFP.*
- **Riesgo residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente. *Fuente: Anexo glosario de la Guía para la Gestión Integral del Riesgo en Entidades Públicas V7, 2025. 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 Integrado de Gestión de Riesgos:** comprende el marco y proceso estructurado para la identificación, análisis, valoración, priorización según aplique, establecimiento e implementación de tratamientos o estrategias, y el monitoreo de los riesgos que pueden afectar el cumplimiento de sus objetivos estratégicos y la operación de los procesos. *Fuente: Subdirección de Procesos*
- **TAC:** Tributario, Aduanero y Cambiario.
- **Tratamiento:** consiste en seleccionar e implementar opciones para abordar el riesgo, como, por ejemplo, controles, estrategias, planes de acción, protocolos, entre otros). *Fuente: basado en la norma NTC ISO 31000:2018. Gestión de riesgos.*

11. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	21/08/2020	02/10/2023	Versión inicial. Se denomina “Marco para la gestión de riesgos en la Dirección de Impuestos y Aduanas Nacionales” e incluye la Política de gestión de riesgos, principios, responsabilidades, información, comunicación y reporte de la gestión de riesgos. Conforme con el artículo 4 del Decreto	

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

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
			648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, la actualización de la Política de administración del riesgo fue aprobada en sesión del Comité Institucional de Coordinación de Control Interno de la UAE DIAN el 21/08/2020.	
2	03/10/2023	03/12/2024	Versión 2 que reemplaza lo establecido en la versión 1. Se realizan ajustes de acuerdo con los lineamientos metodológicos de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 del Departamento Administrativo de la Función Pública DAFP, 2022. Se cambia el nombre a “Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN”. Se establecen lineamientos para el Sistema de Gestión de Riesgos Institucionales, en los que se incluyeron: • Riesgos estratégicos, operacionales, de capital humano, de seguridad y salud en el trabajo, ambientales, de seguridad de la información, de fraude y corrupción y fiscales. No se abordan lineamientos para los riesgos de Cumplimiento TAC, pero se hace referencia a su existencia. Conforme con el artículo 4 del Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015,	

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

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
			Reglamentario Único del Sector de la Función Pública, la actualización de la Política de administración del riesgo fue aprobada en sesión del Comité Institucional de Coordinación de Control Interno de la UAE DIAN el 03/10/2023.	
3	04/12/2024	15/06/2026	Versión 3 que reemplaza lo establecido en la versión 2. Se amplía el alcance para el Sistema de Gestión de Riesgos, en los que se incluyeron y desarrollaron lineamientos para los riesgos de cumplimiento Tributario, Aduanero y Cambiario TAC y riesgos de lavado de activos, financiación del terrorismo y financiación para la proliferación de armas de destrucción masiva – LA/FT/FP. Así mismo, se cambia el nombre de riesgos de fraude y corrupción por riesgos de integridad. Conforme con el artículo 4 del Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, la actualización de la Política de administración del riesgo fue aprobada en sesión del Comité Institucional de Coordinación de Control Interno de la UAE DIAN el 04/12/2024.	Pública
4	16/06/2026		Versión 4 que reemplaza lo establecido en la versión 3. Se realizan ajustes de acuerdo con los lineamientos metodológicos	Pública

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
			actualizados en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 del Departamento Administrativo de la Función Pública DAFP, 2025. Estos ajustes están relacionados con el despliegue de riesgos para la integridad, principalmente en lo asociado al lavado de activos, financiación del terrorismo y financiación para la proliferación de armas de destrucción masiva – LA/FT/FP. Se incluyen lineamientos frente a la continuidad del negocio en la entidad. Inclusión de lineamientos para ejercer la función de cumplimiento. Conforme con el artículo 4 del Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, la actualización de la Política de administración del riesgo fue aprobada en sesión del Comité Institucional de Coordinación de Control Interno de la UAE DIAN el 16 de junio 2026	