

OFICINA ASESORA DE PLANEACIÓN Y COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

**DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA – DANE y
FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO NACIONAL
DE ESTADÍSTICA – FONDANE**

NOVIEMBRE DE 2020



**El futuro
es de todos**

**Gobierno
de Colombia**

CONTENIDO

1. Introducción	4
2. Marco normativo	5
3. Política de administración de riesgos	7
3.1 Compromiso de la Alta Dirección	7
3.2 Objetivo	7
3.3 Alcance	7
3.4 Gobernanza de la administración de riesgos	7
3.4.1 Línea estratégica	8
3.4.2 Primera línea de defensa	10
3.4.3 Segunda línea de defensa	12
3.4.4 Tercera línea de defensa	15
3.5 Mapa de calor, niveles de aceptación del riesgo y acciones de tratamiento	17
4. Glosario	19
Bibliografía	21

Lista de tablas

Tabla 1. Roles y responsabilidades de la línea estratégica (instancia decisoria)	9
Tabla 2. Roles y responsabilidades de la primera línea de defensa	10
Tabla 3. Roles y responsabilidades de la segunda línea de defensa	13
Tabla 4. Roles y responsabilidades de la tercera línea de defensa	15
Tabla 5. Niveles de aceptación del riesgo y acciones de tratamiento.....	18

Lista de imágenes

Imagen 1. Esquema de gobernanza de la administración del riesgo	8
Imagen 2. Mapa de calor.....	18

1. Introducción

El Departamento Administrativo Nacional de Estadística – DANE es la entidad de carácter técnico-científico que se encarga de la planeación, levantamiento, procesamiento, análisis y difusión de las estadísticas oficiales del país y realiza investigaciones de todos los sectores de la economía, industria, población, sector agropecuario y calidad de vida, entre otras; adicionalmente es el ente rector del Sistema Estadístico Nacional, condición que le otorga, entre otras responsabilidades, las de formular y hacer seguimiento a la ejecución del Plan Estadístico Nacional, elaborar, en coordinación con los integrantes del SEN, diagnósticos y planes de fortalecimiento e innovación de registros administrativos para su aprovechamiento estadístico y formular, en coordinación con los integrantes del SEN, estrategias para la innovación en la producción y difusión de las estadísticas oficiales requeridas en el país¹.

Uno de los objetivos del DANE es garantizar la producción, disponibilidad y calidad de la información estadística², la cual es un bien público; por su parte, el Fondo Rotatorio del DANE – FONDANE es la entidad operativa encargada de manejar los recursos para apoyar y financiar el desarrollo de los programas tecnológicos que las normas vigentes le han asignado al DANE, con el propósito de contribuir al desarrollo económico, social y tecnológico del país³.

El servicio prestado por el DANE, de producir y comunicar la información estadística que soporte la comprensión y solución de las problemáticas sociales, económicas y ambientales del país, para que sirvan de base para la toma de decisiones públicas y privadas y contribuyan a la consolidación de un Estado Social de Derecho equitativo, productivo y legal, está catalogado en el proyecto del Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, como un servicio esencial. En consecuencia, el Centro de datos del DANE es considerado infraestructura crítica cibernética, lo que implica que la entidad debe cumplir con lo señalado en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital y en la Guía de Orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, Territoriales y Sector Público, en lo relacionado con los reportes que se deben realizar al Comando Conjunto Cibernético (CCOC) o a la entidad que haga sus veces.

El presente documento contiene los lineamientos y prácticas a seguir en torno a la identificación, valoración, tratamiento y seguimiento de los riesgos de gestión, de corrupción y de seguridad de la información (los cuales incluyen riesgos de seguridad digital), que pueden presentarse en los programas, proyectos o procesos del DANE – FONDANE, constituyendo así una política de

¹ Decreto 2404 de 2019, por el cual se reglamenta artículo 155 de la Ley 1955 de 2019 y se modifica el Título 3 de la Parte 2 del Libro 2 del Decreto 1170 de 2015 Único del Sector Administrativo de Información Estadística.

² Decreto 262 de 2004, por el cual se modifica la estructura del Departamento Administrativo Nacional de Estadística DANE y se dictan otras disposiciones.

³ Decreto 590 de 1991, por el cual se reorganiza la administración y manejo del Fondo Rotatorio del Departamento Administrativo Nacional de Estadística - FONDANE.

administración de riesgos. Esta política está elaborada con base en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4 (2018); en el anexo 4 de la mencionada guía, el cual contiene los lineamientos para la gestión de riesgos de seguridad digital en Entidades Públicas; y en la Guía de orientación para la gestión de riesgos de seguridad digital en el Gobierno Nacional, Territoriales y Sector Público.

Esta política es la base para el desarrollo de un conjunto de actividades de identificación y valoración de los riesgos, las cuales conforman un esquema con enfoque preventivo que brinda una seguridad razonable frente al logro de los objetivos institucionales, y debe ser aplicada por todos los servidores públicos y contratistas que realizan actividades para el DANE y FONDANE.

2. Marco normativo

El ordenamiento jurídico colombiano contiene varias disposiciones normativas que regulan la administración de riesgos:

La Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones, indica en su artículo 2, los objetivos del sistema de control interno; entre éstos se encuentran el de proteger los recursos de la organización de los posibles riesgos que los afecten, así como definir y aplicar medidas para prevenir los riesgos y detectar y corregir las desviaciones que puedan afectar el logro de sus objetivos; y el artículo 4 de la citada Ley, establece que toda entidad debe definir políticas como guías de acción y procedimientos para la ejecución de los procesos.

El Decreto 1537 de 2001, que reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado, indica en su artículo 4 la obligatoriedad para las entidades públicas de establecer y aplicar políticas de administración del riesgo; en este sentido, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, mediante el cual se evalúan los aspectos tanto internos como externos que pueden llegar a representar una amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones de control y prevención efectivas, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.

La Ley 1474 de 2011, que dicta normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, en su artículo 73 establece la obligatoriedad de elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano, la cual contempla el mapa de riesgos de corrupción y medidas concretas para mitigarlos.

El Decreto 1083 de 2015, mediante el cual se expide el Decreto único reglamentario del Sector de Función Pública, indica en el artículo 2.2.21.5.4, la obligatoriedad que tienen las entidades públicas de establecer y aplicar políticas de administración del riesgo y en el literal g del artículo 2.2.21.1.6, establece que el Comité Institucional de Coordinación de Control Interno debe someter a aprobación del representante legal, la política de administración de riesgos y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta. En concordancia, la Resolución 683 de 2018 del DANE – FONDANE establece en el numeral 7 del artículo 2, que una de las funciones del Comité de Coordinación de Control Interno es someter a aprobación del representante legal del DANE y FONDANE la política de administración de riesgos y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

El Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, único reglamentario del sector función pública, en su artículo 4 adiciona al artículo 2.2.21.1.6 del Decreto 1083 de 2015, la función del Comité Institucional de Coordinación de Control Interno, de someter a aprobación del representante legal la política de administración de riesgos y hacer seguimiento, en especial a la prevención y detección del fraude y mala conducta.

El Decreto 1499 de 2017, que modifica el Decreto 1083 de 2015, único reglamentario del sector función pública en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015, en su artículo 1 indica que mediante el artículo 2.2.22.3.1 del Decreto 1083 de 2015, se adopta la versión actualizada del Modelo Integrado de Planeación y Gestión – MIPG; la dimensión No. 7 de este documento, que se refiere al control interno, establece que a partir de la política de administración de riesgos se deben establecer sistemas de gestión de riesgos y las responsabilidades para controlarlos.

El CONPES 3854 del 11 de abril de 2016, que estableció la política nacional de Seguridad Digital, busca fortalecer las capacidades de las entidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsa una mayor prosperidad económica y social en el país.

El CONPES 3995 del 01 de julio de 2020, que instaura la Política Nacional de Confianza y Seguridad Digital, busca establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital, de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Del marco jurídico expuesto anteriormente, se desprende la obligación del DANE y el FONDANE, de adoptar una política para la administración de los riesgos.

3. Política de administración de riesgos

3.1 Compromiso de la Alta Dirección

La Alta Dirección⁴ del DANE y del FONDANE se compromete a administrar los riesgos de gestión, de corrupción y de seguridad de la información, estableciendo lineamientos que orienten el direccionamiento estratégico y la gestión institucional a evitar su materialización, de forma que se asegure el rigor y la calidad en la producción estadística; así mismo, a asignar los recursos pertinentes que se requieran para la prevención y el tratamiento adecuado de los riesgos.

3.2 Objetivo

Establecer la gobernanza de la administración de los riesgos de gestión, de corrupción y de seguridad de la información del DANE y del FONDANE, procurando asegurar el cumplimiento de los objetivos institucionales y mejorar el desempeño de los procesos.

3.3 Alcance

Los lineamientos contenidos en la presente política, aplican para la administración de los riesgos de gestión, de corrupción y de seguridad de la información del DANE-FONDANE. Los riesgos de seguridad y salud en el trabajo, los ambientales y los de procesos de contratación se excluyen del alcance de la presente política, puesto que deben ser administrados por los respectivos responsables teniendo en cuenta la normatividad y las metodologías propias que los rigen.

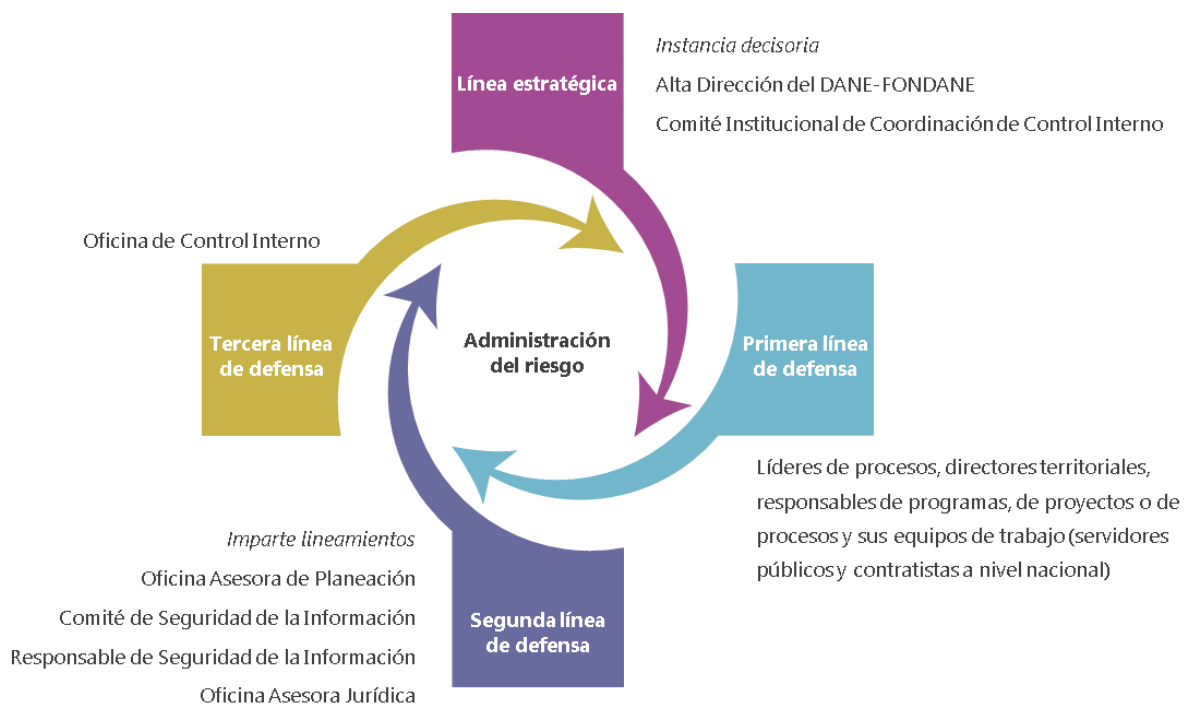
3.4 Gobernanza de la administración de riesgos

La gobernanza de la administración de los riesgos implica la definición de una serie de lineamientos que permiten orientar el actuar de las distintas líneas de defensa en torno a la prevención y tratamiento de los riesgos e involucra a todos los servidores públicos y contratistas del DANE y FONDANE.

Esta gobernanza opera bajo un modelo de líneas defensa, el cual establece los roles y responsabilidades de todos los actores entorno a la administración de riesgos.

La siguiente imagen representa el esquema de gobernanza de la administración del riesgo en el DANE-FONDANE:

⁴ La Alta Dirección en el DANE es el Director y Representante legal de FONDANE.

Imagen 1. Esquema de gobernanza de la administración del riesgo

A continuación, se relacionan los roles y responsabilidades de cada una de las líneas de defensa. Las responsabilidades obedecen a acciones, las cuales pueden ser de tres tipos: preventivas recurrentes (indicadas con color verde), preventivas para evitar la materialización de riesgos (color naranja) y correctivas para mitigar los riesgos materializados (color azul).

3.4.1 Línea estratégica

La línea estratégica para la administración de los riesgos está conformada por la alta dirección de la Entidad y el Comité Institucional de Coordinación de Control Interno. Sus roles y responsabilidades son los siguientes:

Tabla 1. Roles y responsabilidades de la línea estratégica (instancia decisoria)

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción
Alta Dirección	Revisar, ajustar de ser necesario y aprobar la política de administración de riesgos.	Mínimo cada dos años y cada vez que se requiera.	Política de administración de riesgos.	
	<p>Tomar decisiones y asignar recursos disponibles para la administración del riesgo a partir de:</p> <ul style="list-style-type: none"> Los cambios identificados en el direccionamiento estratégico y en el contexto de la entidad, y advertir a la primera línea de defensa la forma en que estos cambios pueden tener un impacto significativo en la operación de la entidad y generar cambios en la estructura de riesgos y controles. Los reportes de monitoreo de riesgos elaborados por la segunda y los informes seguimiento de riesgos elaborados por la tercera línea de defensa. Informes de seguimiento a planes de tratamiento y de mejoramiento, elaborados por la tercera línea de defensa. Los niveles de aceptación del riesgo. 	Mínimo cada cuatro meses y cada vez que se requiera.	<p>Contexto estratégico.</p> <p>Planeación estratégica.</p> <p>Reportes de monitoreo e informes de seguimiento de riesgos.</p> <p>Política de administración de riesgos.</p>	
Comité Institucional de Coordinación de Control Interno	Someter a aprobación del representante legal del DANE y del FONDANE, la política de administración de riesgos y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta. (Resolución 0683 de 2018).	Mínimo cada dos años y cada vez que se requiera.	Política de administración de riesgos.	

Fuente: Adaptado de Departamento Administrativo de la Función Pública (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas (p. 77).

3.4.2 Primera línea de defensa

La primera línea de defensa está conformada por los líderes de procesos, directores territoriales, responsables de programas, de proyectos o de procesos y sus equipos de trabajo (servidores públicos y contratistas a nivel nacional). Sus roles y responsabilidades son los siguientes:

Tabla 2. Roles y responsabilidades de la primera línea de defensa

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción	
Líderes de procesos, directores territoriales, responsables de programas, de proyectos o de procesos y sus equipos de trabajo (servidores públicos y contratistas a nivel nacional)	Identificar los cambios en el direccionamiento estratégico y en el contexto de la entidad y cómo estos pueden generar nuevos riesgos o modificar los existentes en sus procesos.	Mínimo cada cuatro meses y cada vez que se requiera.	Contexto estratégico. Planeación estratégica. Mapa de riesgos.		
	Identificar, actualizar, analizar, valorar y monitorear los riesgos (de gestión, de corrupción y de seguridad de la información), conforme con los lineamientos para la administración del riesgo. * Los riesgos pueden presentarse en los programas, proyectos o procesos del DANE – FONDANE. * Los riesgos que puedan generar daño antijurídico serán tratados como riesgos de gestión.	Mínimo cada cuatro meses y cada vez que se requiera. La actualización de los riesgos se realiza cada vez que se requiera.	Contexto estratégico. Política de prevención del daño antijurídico del DANE-FONDANE. Documentación para la administración de riesgos. Mapa de riesgos.		
	Definir, documentar, ejecutar y actualizar los controles que minimicen las vulnerabilidades y prevengan el daño antijurídico. Asegurar que los controles sean ejecutados oportuna y eficazmente por personal idóneo y competente. Hacer seguimiento al diseño y ejecución de los controles y determinar si son efectivos y adecuados para contrarrestar las vulnerabilidades. En caso de que se detecten deficiencias en los controles, determinar y ejecutar las acciones de mejora a que haya lugar. Recopilar las evidencias de la ejecución de los controles y tenerlas a disposición para presentarlas cuando	La definición, documentación o actualización de los controles se realiza cada vez que se identifican o se ajustan los mapas de riesgos. La ejecución de controles y disposición de evidencias se realiza de acuerdo con su periodicidad. El seguimiento se realiza mínimo cada cuatro meses y cada vez que se requiera.	Política de prevención del daño antijurídico del DANE-FONDANE. Documentación para la administración de riesgos. Mapa de riesgos.		

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción
	sean requeridas.			
	<p>Tomar decisiones conjuntamente con la alta dirección con respecto al tratamiento a dar a los riesgos según el nivel de aceptación de los mismos.</p> <p>Reportar a la segunda línea de defensa el monitoreo de los riesgos, incluyendo el reporte de riesgos materializados y los incidentes de seguridad digital.</p> <p>* Si se materializa un riesgo de gestión, de corrupción o de seguridad de la información, es necesario revisar y ajustar en lo pertinente, el mapa de riesgos del respectivo proceso.</p> <p>* Si se detecta la materialización de un riesgo de corrupción, debe:</p> <ul style="list-style-type: none"> • Informar al superior inmediato sobre el hecho encontrado. • Denunciar el caso ante la Oficina de Control Interno Disciplinario. <p>* Los riesgos de gestión y de corrupción materializados se reportan a la Oficina Asesora de Planeación.</p> <p>* Los riesgos de seguridad de la información materializados o los incidentes de seguridad deben ser informados al responsable de seguridad de la información o a quien haga sus veces.</p> <p>* Los riesgos materializados catalogados como extremos o altos deben ser adicionalmente reportados de manera inmediata a la línea estratégica.</p>	<p>La toma de decisiones con respecto al tratamiento a dar los riesgos y el monitoreo se realizan mínimo cada cuatro meses y cada vez que se requiera.</p> <p>El reporte de los riesgos materializados se realiza tan pronto como ocurran.</p>	<p>Política de administración de riesgos.</p> <p>Documentación para la administración de riesgos.</p> <p>Mapa de riesgos.</p>	
	Formular, ejecutar, hacer seguimiento y determinar la efectividad de los planes de tratamiento de los riesgos, conforme con los niveles de aceptación del riesgo.	Cada vez que se requiera.	Formato de plan de mejoramiento.	

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción
	Formular, ejecutar, hacer seguimiento y determinar la efectividad de los planes de mejoramiento para evitar que los riesgos materializados vuelvan a ocurrir. * Para formular planes de mejoramiento, se deben tener en cuenta las decisiones tomadas en los Comités de Coordinación de Control Interno y de Seguridad de la Información, así como las recomendaciones de la Oficina Asesora de Planeación, de la Oficina de Control Interno y del responsable de seguridad de la información o quien haga sus veces.	Cada vez que se requiera.	Formato de plan de mejoramiento.	
	Aprobar los mapas de riesgos de los procesos a su cargo y asegurar su socialización e implementación en donde aplique.	Cada vez que se elaboren y actualicen.	Mapa de riesgos.	
	Elaborar y actualizar el inventario de activos de información de los procesos a su cargo.	Anualmente.	Metodología para la identificación, clasificación y valoración de activos de información.	

Fuente: Adaptado de Departamento Administrativo de la Función Pública (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas (p. 78).

3.4.3 Segunda línea de defensa

La segunda línea de defensa está conformada por la Oficina Asesora de Planeación, el Comité de Seguridad de la Información, el responsable de seguridad de la información y la Oficina Asesora Jurídica. Sus roles y responsabilidades son los siguientes:

Tabla 3. Roles y responsabilidades de la segunda línea de defensa

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción
Oficina Asesora de Planeación y Comité de Seguridad de la Información	Liderar, diseñar e impartir lineamientos para implementar la estrategia de administración de riesgos, en coordinación con las demás líneas de defensa.	Cada vez que se requiera	Lineamientos o referentes del Departamento Administrativo de la Función Pública – DAFP. Lineamientos o referentes para la Gestión de Riesgos de Seguridad Digital - Ministerio de Tecnologías de Información y Comunicaciones - MinTic. Política de administración de riesgos. Documentación para la administración de riesgos. Mapa de riesgos.	
	Definir o actualizar y socializar la política de administración de riesgos.	Mínimo cada dos años y cada vez que se requiera.	Lineamientos o referentes del Departamento Administrativo de la Función Pública – DAFP. Lineamientos o referentes para la Gestión de Riesgos de Seguridad Digital - Ministerio de Tecnologías de Información y Comunicaciones - MinTic. Política de administración de riesgos.	
	Establecer, actualizar y socializar documentación para la administración de riesgos.	Cada vez que se requiera.	Lineamientos o referentes del Departamento Administrativo de la Función Pública – DAFP. Lineamientos o referentes para la Gestión de Riesgos de Seguridad Digital - Ministerio de Tecnologías de Información y Comunicaciones - MinTic. Política de administración de riesgos. Documentación para la administración de riesgos.	

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción
Comité de Seguridad de la Información	Definir y actualizar de ser necesario, la metodología para la identificación, clasificación y valoración de activos de información para aprobación de la Alta Dirección.	Cada vez que se requiera.	Lineamientos o referentes para la Gestión de Riesgos de Seguridad Digital - Ministerio de Tecnologías de Información y Comunicaciones - MinTic.	
Oficina Asesora de Planeación y Responsable de seguridad de la información	Asesorar de forma proactiva a la primera línea de defensa en el análisis de cambios en el direccionamiento estratégico y en el contexto de la entidad, así como en la identificación, actualización, valoración y monitoreo de los riesgos.	La actualización de los riesgos de corrupción se realiza cada año y cada vez que se requiera. La actualización de los riesgos de gestión y de seguridad de la información se realiza cada vez que se requiera.	Lineamientos o referentes del Departamento Administrativo de la Función Pública – DAFP. Lineamientos o referentes para la Gestión de Riesgos de Seguridad Digital - Ministerio de Tecnologías de Información y Comunicaciones - MinTic. Contexto estratégico. Planeación estratégica. Política de administración de riesgos. Documentación para la administración de riesgos. Mapa de riesgos.	
	Realizar recomendaciones para el adecuado diseño, documentación y fortalecimiento de los controles.	Las recomendaciones para el diseño y fortalecimiento de los controles se realizan cada vez que se requiera.		
	Elaborar reportes cuatrimestrales para la Línea estratégica sobre los riesgos, su severidad y materialización.	Mínimo cada cuatro meses y cada vez que se requiera.	Mapa de riesgos.	
	Asesorar a la primera línea de defensa en la formulación de planes de tratamiento y de mejoramiento.	Cada vez que se requiera.	Mapa de riesgos. Procedimiento para la elaboración, suscripción y seguimiento a planes de mejoramiento integrados.	
Responsable de seguridad de la información	Asesorar en la identificación y valoración de los activos de información.	Anualmente y cada vez que se requiera.	Metodología para la identificación, clasificación y valoración de activos de información.	
	Reportar a la línea estratégica los incidentes de seguridad y los resultados de los indicadores de desempeño para la gestión de riesgos de seguridad de la	Mínimo cada cuatro meses y cada vez que se requiera.	Documentación para la administración de riesgos. Mapa de riesgos.	

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción
	información.			
	Convocar de manera extraordinaria al Comité de Seguridad de la Información cuando se materialice un riesgo de seguridad de la información o un incidente de seguridad.	Cada vez que se requiera.	Documentación para la administración de riesgos. Mapa de riesgos.	
Oficina Asesora Jurídica	Asesorar a la primera línea de defensa en el establecimiento de controles adecuados para minimizar las vulnerabilidades que puedan generar daño antijurídico.	Cada vez que se requiera.	Política de prevención del daño antijurídico del DANE-FONDANE.	

Fuente: Adaptado de Departamento Administrativo de la Función Pública (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas (p. 79).

3.4.4 Tercera línea de defensa

La tercera línea de defensa está conformada por la Oficina de Control Interno. Sus roles y responsabilidades son los siguientes:

Tabla 4. Roles y responsabilidades de la tercera línea de defensa

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción
	Evaluar el cumplimiento y recomendar mejoras sobre la implementación de la política de administración de riesgos.	Mínimo cada cuatro meses y cada vez que se requiera.	Política de administración de riesgos. Documentación para la administración de riesgos. Mapa de riesgos.	
Oficina de Control Interno	Revisar cambios en el direccionamiento estratégico y en el contexto de la entidad que pueden generar nuevos riesgos o modificar los que ya se tienen identificados en los procesos, con el fin de solicitar a la primera línea de defensa la actualización de los riesgos.	Mínimo cada cuatro meses y cada vez que se requiera.	Contexto estratégico. Planeación estratégica. Documentación para la administración de riesgos. Mapa de riesgos.	

Quién	Qué hace	Cuándo lo hace	Herramientas	Tipo de acción
	Revisar que se hayan identificado los riesgos significativos que afectan el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.	Mínimo cada cuatro meses y cada vez que se requiera.	Contexto estratégico. Planeación estratégica. Documentación para la administración de riesgos. Mapa de riesgos.	
	Elaborar informes periódicos para la línea estratégica, que den cuenta de la evaluación independiente sobre la efectividad del sistema de administración de riesgos. Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad no sea coherente con los resultados de las auditorías realizadas.	Mínimo cada cuatro meses y cada vez que se requiera.	Documentación para la administración de riesgos. Mapa de riesgos.	
	Revisar el adecuado diseño, ejecución y documentación de los controles que se han establecido por parte de la primera línea de defensa.	Mínimo cada cuatro meses y cada vez que se requiera.	Documentación para la administración de riesgos. Mapa de riesgos.	
	Asesorar y presentar recomendaciones con enfoque preventivo a la primera línea de defensa de forma coordinada con la segunda línea de defensa sobre la identificación y monitoreo de los riesgos y el diseño de controles.	Mínimo cada cuatro meses y cada vez que se requiera.	Documentación para la administración de riesgos. Mapa de riesgos.	
	Revisar y realizar seguimiento a los planes de tratamiento o de mejoramiento suscritos por la primera línea de defensa para determinar su cumplimiento y efectividad y presentar los informes respectivos a la alta dirección.	Cada vez que se requiera.	Planes de tratamiento o de mejoramiento suscritos por la primera línea de defensa. Procedimiento para la elaboración, suscripción y seguimiento a planes de mejoramiento integrados.	

Fuente: Adaptado de Departamento Administrativo de la Función Pública (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas (p. 80).

3.5 Mapa de calor, niveles de aceptación del riesgo y acciones de tratamiento

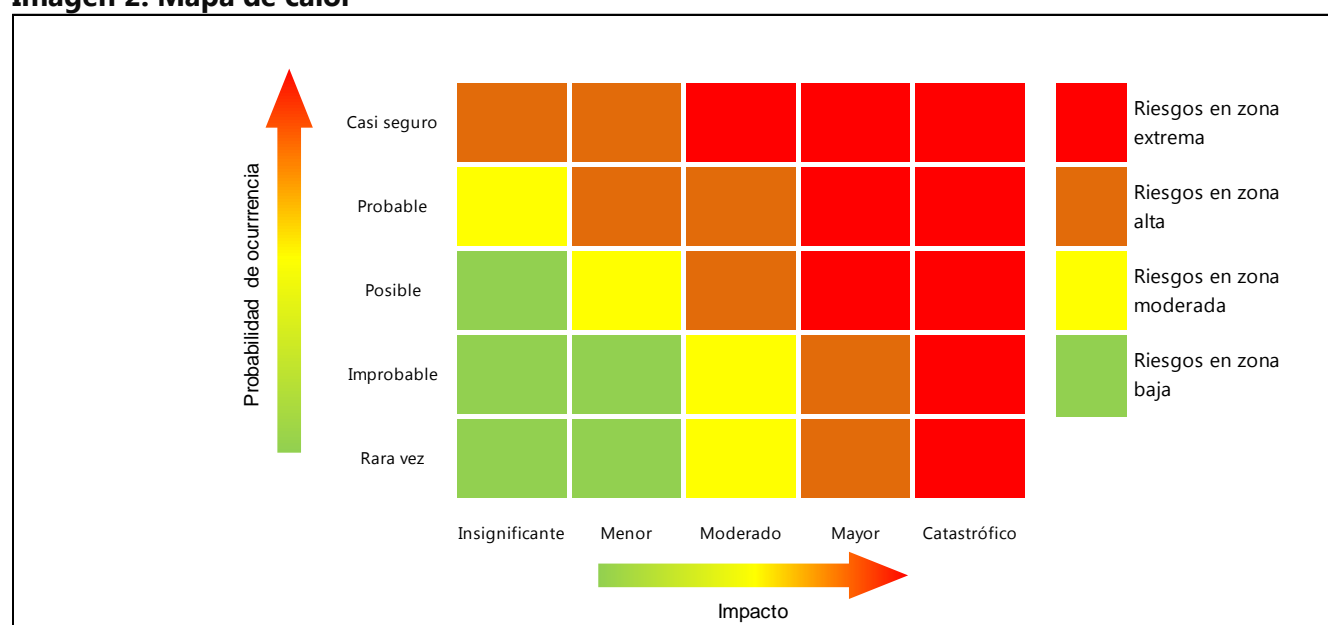
Los riesgos pueden ser tratados con las siguientes acciones o con una combinación de las mismas:

- **Aceptar el riesgo:** Aceptar los riesgos residuales implica que dado que su probabilidad de ocurrencia es baja y que su impacto es insignificante, se puede tratar con los controles existentes; en este sentido, NO es necesario adoptar ninguna medida que afecte la probabilidad o el impacto del riesgo; simplemente se deben seguir aplicando los controles existentes y realizar monitoreo para evitar que el riesgo que alcance un nivel mayor. Es de anotar que los riesgos de corrupción no se aceptan en ningún caso.
- **Reducir el riesgo:** Los riesgos residuales se reducen formulando acciones preventivas adicionales y diferentes a los controles, con el fin de minimizar la probabilidad de ocurrencia o el impacto del riesgo o ambos y de que se fortalezcan los puntos débiles o fallas identificadas en el diseño y en la evaluación de los controles. Si al realizar la valoración de los riesgos se establece que no existen controles implementados, estas acciones preventivas deben estar dirigidas justamente a que se implementen nuevos controles.
- **Compartir o transferir el riesgo:** El riesgo residual, o una parte de este, puede ser transferido a, o compartido con otros grupos de interés que puedan gestionarlo con más eficacia cuando no sea posible reducirlo a un nivel aceptable; es de anotar que no es posible transferir la responsabilidad del riesgo. Las formas más comunes de compartir o transferir un riesgo son los seguros o tercerización, los cuales deben respaldarse con un acuerdo contractual.
- **Evitar el riesgo:** Implica no iniciar o no continuar con las actividades que causan el riesgo.

Estas acciones aplican para los riesgos residuales, los cuales son aquellos que permanecen después de establecer y evaluar los controles que contribuyen a minimizar su probabilidad de ocurrencia e impacto.

Para determinar la acción a seguir, es necesario tener en cuenta que la combinación de probabilidad e impacto de los riesgos determina qué tan aceptables pueden ser. Los criterios para determinar la probabilidad de ocurrencia y el impacto de los riesgos se encuentran establecidos en la documentación para la administración del riesgo complementaria a esta política. La combinación de probabilidad e impacto se representa gráficamente en un mapa de calor. El DANE – FONDANE adopta el mapa de calor establecido por el DAFP, en la Guía para la administración del riesgo y el diseño de controles en las entidades públicas (2018), el cual se muestra a continuación:

Imagen 2. Mapa de calor



Fuente: Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas (p. 47).

La zona del mapa en donde se ubiquen los riesgos determina su nivel de aceptación y permite establecer las acciones de tratamiento, así como los recursos y esfuerzos necesarios para mitigar sus posibles impactos. Las decisiones tomadas por la Línea estratégica y por la primera línea de defensa se basarán en los criterios que se indican en la siguiente tabla:

Tabla 5. Niveles de aceptación del riesgo y acciones de tratamiento

Zona de riesgo	Acciones de tratamiento
Extrema	<p>Los riesgos residuales ubicados en la zona extrema se pueden materializar en cualquier momento, con efectos catastróficos y por lo tanto se deben evitar; si esto no es posible, se puede optar por reducirlo, compartirlo o transferirlo.</p> <p>Si se decide reducir, se deben formular planes de tratamiento con acciones preventivas inmediatamente (máximo dentro de los 10 días hábiles siguientes a la entrada en vigencia del mapa de riesgos). Estas acciones no deben superar el plazo de un año para su ejecución.</p> <p>El reporte de estos riesgos debe ser conocido por la Línea estratégica, puesto que su tratamiento puede implicar la toma de decisiones o la asignación de recursos adicionales.</p> <p>Si el tratamiento de estos riesgos implica el desarrollo de acciones a nivel institucional, la primera línea de defensa debe tomar decisiones conjuntamente con la línea estratégica.</p>

Zona de riesgo	Acciones de tratamiento
Alta	<p>Los riesgos residuales ubicados en la zona alta se deben evitar; si esto no es posible, se puede optar por reducirlo, compartirlo o transferirlo.</p> <p>Si se decide reducir, se deben formular planes de tratamiento con acciones preventivas (máximo dentro del mes siguiente a la entrada en vigencia del mapa de riesgos). Estas acciones no deben superar el plazo de un año para su ejecución.</p> <p>El reporte de estos riesgos debe ser conocido por la Línea estratégica, puesto que su tratamiento puede implicar la toma de decisiones o la asignación de recursos adicionales.</p> <p>Si el tratamiento de estos riesgos implica el desarrollo de acciones a nivel institucional, la primera línea de defensa debe tomar decisiones conjuntamente con la línea estratégica.</p>
Moderada	<p>Los riesgos residuales ubicados en la zona moderada requieren acciones para reducirlos lo cual implica la formulación de planes de tratamiento con acciones preventivas (máximo dentro de los dos meses siguientes a la entrada en vigencia del mapa de riesgos).</p> <p>Si el tratamiento de estos riesgos implica el desarrollo de acciones a nivel institucional, la primera línea de defensa debe tomar decisiones conjuntamente con la línea estratégica.</p>
Baja	<p>Los riesgos residuales ubicados en la zona baja se pueden aceptar, es decir que se pueden tratar con los controles existentes; en este sentido, NO es necesario adoptar ninguna medida que reduzca la probabilidad o el impacto del riesgo; simplemente se deben seguir aplicando los controles existentes y realizar el monitoreo periódico para evitar que el riesgo alcance un nivel mayor.</p>

Fuente: Adaptado de Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas (p. 68).

4. Glosario

- **Activo:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 2016, pág. 56).
- **Administración del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la entidad un aseguramiento razonable con respecto al logro de los objetivos. (DAFP 2018).
- **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO/IEC 27000:2016).
- **Centro de datos:** centro de cómputo o de procesamiento que puede estar ubicado dentro de las instalaciones de la entidad o ser soportado en su operación por instalaciones de terceros. (Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia PSPICCN V 1.0. 2019).
- **Consecuencia:** Son 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. (DAFP 2018).

- Contexto: Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. (NTC ISO 31000:2011). Se debe establecer el contexto tanto interno como externo de la entidad, además del contexto del proceso del proceso y sus activos de seguridad digital.
- Control: Medida que modifica el riesgo. (NTC ISO 31000:2011). Medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. (MGRSD 2018).
- Daño antijurídico: Perjuicio causado a una persona natural o jurídica, como consecuencia de una acción, omisión o exceso en el ejercicio de una actividad pública, que provoque que el afectado soporte una carga u obligación, superior a la que social o legalmente estaba obligado.
- Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad. (DAFP 2018).
- Gobernanza: Arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía (RAE). En su marco de políticas para una buena gobernanza pública, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), define este concepto como "la formulación, la ejecución y la evaluación de reglas, procesos e interacciones formales e informales entre las instituciones y los agentes que componen el Estado, y entre el Estado y los ciudadanos, sea individualmente, sea en forma de organizaciones de la sociedad civil, de empresas y de otros agentes no estatales, que enmarquen el ejercicio de la autoridad pública en aras del interés público y una toma de decisiones que permita una adecuada anticipación y detección de problemas y que, en respuesta, sustente el incremento de la prosperidad y del bienestar generales".
- Impacto: Se entiende como las consecuencias ocasionadas por la materialización del riesgo. (DAFP 2018).
- Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).
- Integridad: Propiedad de exactitud y completitud. (DAFP 2018).
- Política de administración de riesgos: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).
- Probabilidad: Es la posibilidad de ocurrencia de un riesgo, la cual puede ser medida con criterios de frecuencia o factibilidad. (DAFP 2018).
- 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. (DAFP 2018).
- Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias. (DAFP 2018).

- 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. (ISO/IEC 27000).
- Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como 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. (DAFP 2018).
- Riesgo inherente: Es aquel al que se enfrenta la entidad en ausencia de controles que modifiquen su probabilidad de ocurrencia o impacto. (DAFP 2018).
- Riesgo residual: Es el riesgo que permanece luego de haber diseñado, implementado y valorado la efectividad de los controles. (Basado en DAFP 2018).
- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27000:2016).
- Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (cibespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854 2016, pág. 29).
- Servicio esencial: Servicio prestado por el gobierno o por cualquier organización o entidad, es aquel servicio cuya modificación o interrupción puede poner en riesgo la seguridad, la salud o la vida de los ciudadanos. (Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia PSPICCN V 1.0. 2019).
- Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas. (Basado en DAFP 2018).

Bibliografía

Departamento Administrativo de la Función Pública (2018). *Guía para la administración del riesgo y el diseño de controles en entidades públicas*. Recuperado de https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499

Ministerio de Tecnologías de la Información y las Comunicaciones. *Modelo nacional de gestión de riesgos de seguridad digital*.

Ministerio de Tecnologías de la Información y las Comunicaciones (2018). *Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas*. Recuperado de <https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+G>

estion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-
+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b?version=1.0

Ministerio de Tecnologías de la Información y las Comunicaciones. *Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, Territoriales y Sector Público.*

Ministerio de Tecnologías de la Información y las Comunicaciones (2016). *Guía de gestión de riesgos de seguridad y privacidad de la información.* Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Consejo Nacional de Política Económica y Social (2016). *Documento CONPES 3854 Política nacional de Seguridad Digital.* Recuperado de <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Consejo Nacional de Política Económica y Social (2020). *Documento CONPES 3995 Política nacional de confianza y seguridad digital.* Recuperado de <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf>