DANE
INFORMACIÓN PARA TODOS

OFICINA ASESORA DE PLANEACIÓN

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

ENERO 2023

INTRODUCCIÓN

Mediante la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el DANE busca establecer medidas para mitigar los riesgos asociados a los activos de información, como la pérdida de confidencialidad, integridad y disponibilidad, procurando así, evitar situaciones que generen incertidumbre en el cumplimiento de la misionalidad de la Entidad.

El presente plan se elabora con el fin de evaluar las acciones que permitan mitigar los riesgos identificados en los procesos de la entidad, estas acciones se encuentran compuestas por actividades que se definen teniendo en cuenta la información obtenida del seguimiento a los riesgos de seguridad y privacidad de la información, las necesidades y el contexto de la entidad; dichas actividades establecen tareas, responsables y fechas de ejecución durante la vigencia.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información se elabora con el fin de dar cumplimiento a lo establecido en el Decreto 612 de 2018 y tiene como base los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la guía de administración de Riesgos y Diseño de Controles, el modelo de Seguridad y Privacidad de la Información-MSPI y el plan de Seguridad y Privacidad de la información, donde se establecen recomendaciones para la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos y los lineamientos de los estándares ISO 27001, ISO 31000:2018.

1. OBJETIVOS

- Cumplir con los requisitos legales, reglamentarios y regulatorios en cuanto a riesgos de Seguridad de la Información.
- Realizar una adecuada gestión de riesgos de Seguridad y Privacidad de la información, teniendo en cuenta los lineamientos establecidos en el DANE.
- Proteger y preservar la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información, mediante la aplicación de los lineamientos establecidos en la Entidad para la gestión de riesgos de Seguridad y Privacidad de la Información, contribuyendo al logro de los objetivos, la misión y la visión institucional.

2. ALCANCE

El Plan de Tratamiento incluye los riesgos de Seguridad de la Información que se encuentren en los niveles moderado, alto y extremo, acorde con los lineamientos definidos en la política de riesgos del DANE, todos aquellos clasificados en niveles inferiores tendrán tratamiento de aceptación por parte de la Entidad. Lo contenido en este plan será aplicable a todos los procesos del DANE.

3. MARCO DE REFERENCIA

3.1. Política de Administración

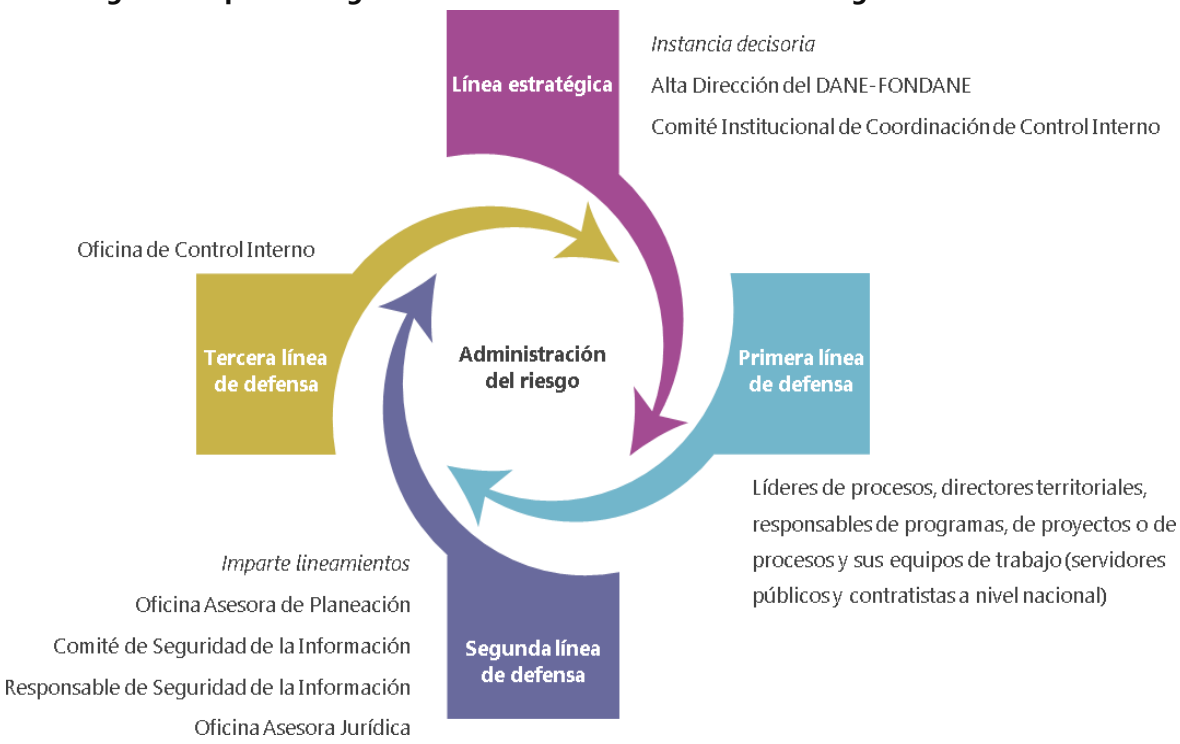
La Alta Dirección del DANE y FONDANE se compromete a administrar los riesgos de gestión, corrupción y seguridad de la información, a través del establecimiento de lineamientos que permitan orientar el direccionamiento estratégico y la gestión institucional, para evitar su materialización, de forma que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

3.2. Gobernanza de la administración de riesgos

La gobernanza de la administración riesgos opera bajo un modelo de líneas defensa, el cual establece los roles y responsabilidades de todos los actores entorno a la administración de riesgos e implica la definición de lineamientos que permiten orientar el actuar de dichas líneas, en torno a la prevención y tratamiento de los riesgos, involucrando a todos los servidores públicos y contratistas del DANE y FONDANE.

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

imagen 1. Esquema de gobernanza de la administración del riesgo



4. METODOLOGÍA

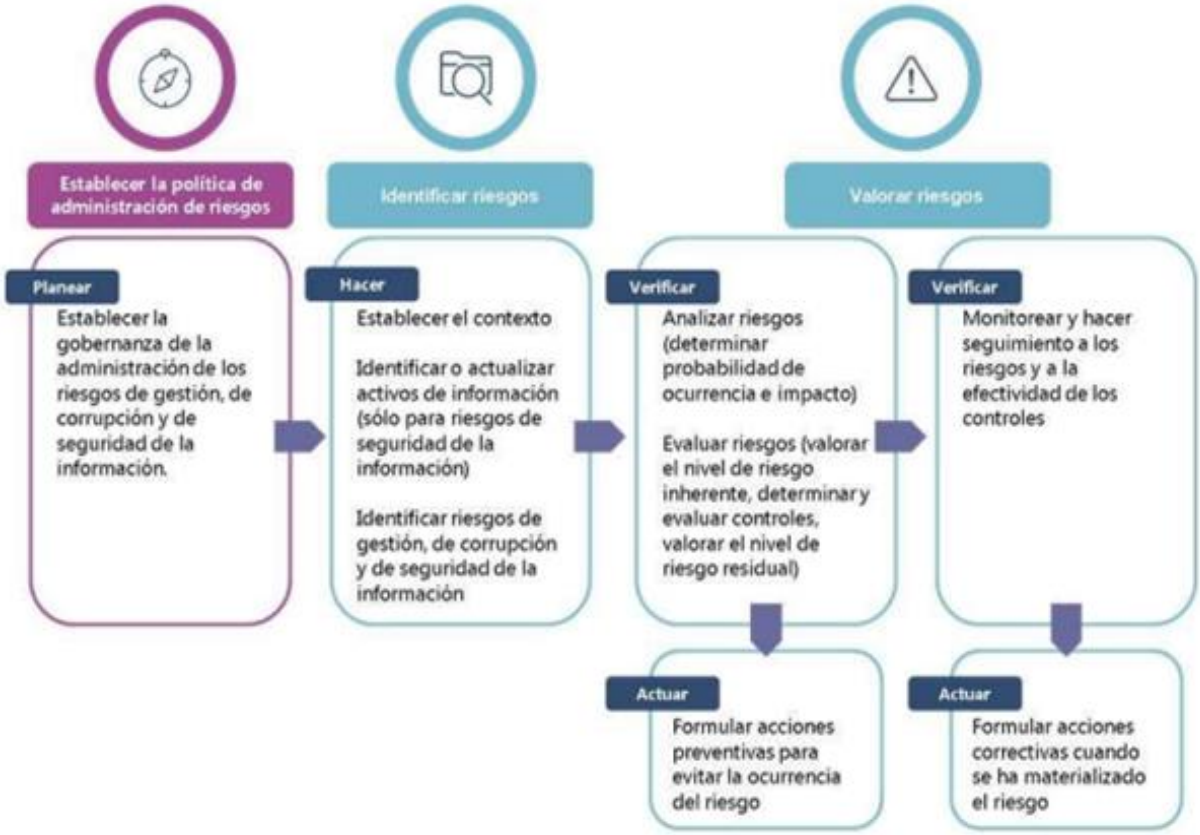
El Plan de Tratamiento de Riesgos de Seguridad de la Información establece las actividades a desarrollar con el fin de mitigar los riesgos sobre los activos identificados por la entidad, de acuerdo con las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información establecida por la Función Pública.

ETAPA	ACTIVIDADES	TAREAS	RESPONSABLE	FECHA INICIO	FECHA FIN
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos.	Oficina Asesora de Planeación	1-feb	31-mar
	Sensibilización	Socializar los lineamientos y Herramientas para la Gestión de los Riesgos de Seguridad y privacidad de la Información.	Oficina Asesora de Planeación	1-mar	30-may

	Identificación de Riesgos de Seguridad y Privacidad de la Información.	Establecer el contexto institucional en relación a la seguridad de la información. (Debilidades, oportunidades, fortalezas y amenazas)	Primera Línea de defensa*	1-mar	31-jul
		Identificar o actualizar los activos de información de los procesos del DANE	Primera Línea de defensa*	10-abr	13-jul
		Identificar, analizar y evaluar los riesgos de seguridad y privacidad de la información	Primera Línea de defensa*	1-mar	31-jul
		Revisar, verificar y retroalimentar los riesgos identificados.	Oficina Asesora de Planeación	1-mar	31-ago
	Aceptación de Riesgos Identificados	Aprobar los riesgos identificados y elaborar los planes de tratamiento cuando aplique.	Líderes de Proceso	1-ago	31-oct
	Seguimiento	Realizar el seguimiento a la implementación de controles y planes de tratamiento para los riesgos identificados.	Todas las líneas de defensa	30-abr	31-ene 2024
	Mejoramiento	Identificar oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento de los riesgos de seguridad y privacidad de la información.	Todos los procesos	30-abr	15-dic
		Revisar o actualizar los lineamientos de Riesgos de Seguridad y privacidad de la información.	Oficina Asesora de Planeación	3-jul	30-dic
		Ajustar los mapas de riesgos de seguridad y privacidad de la información en lo relacionado con controles, vulnerabilidades o responsables.	Todos los procesos	16-ene	22-dic

*Para conocer los Integrantes de las líneas de defensa, revisar el glosario al final del documento.

A continuación, se presenta el gráfico del ciclo de administración de riesgos de la Entidad:



Una vez consolidada la estrategia del manejo de los riesgos de seguridad y privacidad de la información, se identificarán oportunidades que se entenderán como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

5. 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).
- **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).
- **Impacto:** Se entiende como las consecuencias ocasionadas por la materialización del riesgo. (DAFP 2018).
- **Integridad:** Propiedad de exactitud y completitud. (DAFP 2018).
- **Primera línea de defensa:** En el DANE – FONDANE, está conformada por los líderes de procesos, directores territoriales, responsables de programas, de proyectos y sus equipos de trabajo (servidores públicos y contratistas a nivel nacional).
- **Probabilidad:** Es la posibilidad de ocurrencia de un riesgo, la cual puede ser medida con criterios de frecuencia o factibilidad. (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 27000:2016).
- **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).
- **Segunda línea de defensa:** En el DANE – FONDANE, 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.
- **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).
- **Tercera línea de defensa:** En el DANE – FONDANE, está conformada por la Oficina de Control Interno.
- **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).