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

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

enero 2024

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.

1. OBJETIVOS

- Cumplir con los requisitos legales, reglamentarios y regulatorios en cuanto a riesgos de Seguridad y Privacidad 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 e integrantes del nivel directivo de la Entidad se comprometen a administrar los riesgos de gestión, corrupción y fraude, fiscales, de seguridad y privacidad de la información, de los procesos de contratación, 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.

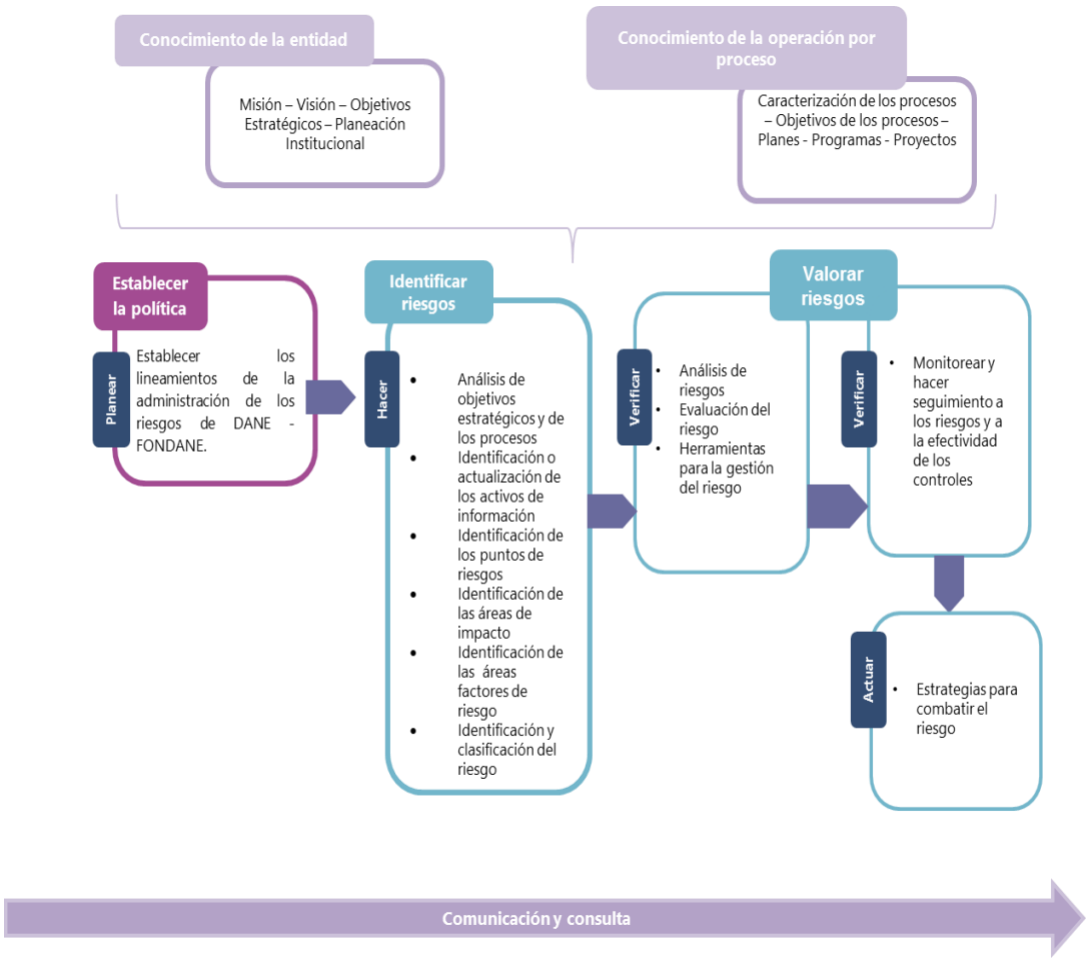
3.2. Metodología para la administración de riesgos

El marco metodológico de la administración de riesgos en el DANE y FONDANE se desarrolla en tres grandes etapas: el establecimiento de la política de administración de riesgos, la identificación de riesgos y la valoración de riesgos, como se muestra en la imagen 1.

Así mismo, las actividades que conforman estas etapas se operativizan a través de documentos y herramientas (procedimientos, guías, formatos) que permiten identificar, valorar y monitorear los riesgos de gestión, de corrupción y fraude, fiscales y de seguridad de la información, que

encuentran dispuestas para consulta en la plataforma tecnológica ISOLUCIÓN https://dane.isolucion.co/frmHome.apx .

Imagen 1. Metodología para la administración de riesgos



Fuente: Adaptado del Departamento Administrativo de la Función Pública. (2022). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6.

3.3. Niveles de autoridad y responsabilidad para la administración de riesgos

La administración de riesgos en la entidad opera bajo un modelo de líneas defensa, el cual establece los roles y responsabilidades que permiten orientar el actuar de este entorno a la prevención y tratamiento de los riesgos. A continuación, se representa el esquema de líneas de defensa:

Imagen 2. Esquema de gobernanza de la administración del riesgo

Fuente: Adaptado del Departamento Administrativo de la Función Pública. (2022). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6

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

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad 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.

Tema	Producto	Responsable	Fecha de inicio	Fecha final
Levantamiento de Activos	FASE I: - Revisión de los activos de información con la identificación, clasificación, valoración de activos de información levantados en los Procesos estratégicos - Procesos de apoyo - Procesos de control y evaluación - Envío de observaciones del levantamiento de activos a los responsables (coordinadores y jefes de áreas) - Ajuste y aprobación de la información sobre los activos de información levantados	Oficina Asesora de Planeación (Oficial de seguridad de la información) - Mesa técnica Jefes de oficina, coordinadores o responsables de las áreas de la entidad relacionando el proceso asociado.	1/02/24	30/04/24
	FASE II: Levantamiento de activos de información con la identificación, clasificación, valoración de activos de información, actualizada (Producción estadística	Oficina Asesora de Planeación (Oficial de seguridad de la información) - Mesa técnica Jefes de oficina, coordinadores o responsables de las áreas de la entidad relacionando el proceso asociado.	1/02/24	31/07/24

Identificación de Riesgos de Seguridad y Privacidad de la Información.	Fase I: - Revisión y ajuste del formato del mapa de riesgos de seguridad y privacidad de la información de acuerdo a la versión 6 de la Guía del DAFP. - Identificación y valoración de riesgos de seguridad de la información, actualizados (Procesos estratégicos, de apoyo, de control y evaluación) - Definir los planes de tratamiento de riesgos de seguridad de la información de los procesos de acuerdo al nivel residual Nota: En el proceso de identificación y valoración, se tendrán en cuenta los riesgos en el tratamiento y protección de datos personales.	Oficial de seguridad de la información y oficial de datos personales Responsables de los procesos y sus delegados	02/05/24	30/08/24
	Fase II: - Identificación y valoración de riesgos de seguridad de la información, actualizados (Proceso Misional. - Producción Estadística) - Definir los planes de tratamiento de riesgos de seguridad de la información del proceso de acuerdo al nivel residual	Oficial de seguridad de la información y oficial de datos personales con los procesos Responsables de los procesos y sus delegados	1/08/24	31/11/2024
Seguimiento	Realizar el seguimiento a la implementación de controles y planes de tratamiento para los riesgos identificados.	Responsables de los procesos y sus delegados Oficial de seguridad de la información y oficial de datos personales Oficina de Control Interno	1/01/24	30/12/24

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).
- 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. (DAFP 2022).
- Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. (DAFP 2022).
- Causa inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituye la causa principal o base para que se presente el riesgo. (DAFP 2022).
- Causa Raíz: Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo. (DAFP 2022).
- Confidencialidad Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados. (DAFP 2022).
- 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.
- 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 2022).
- Control: Medida que permite reducir o mitigar un riesgo. (DAFP 2022).
- 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).
- Factores: de riesgo: Son las fuentes generadoras de riesgos. (DAFP 2022).
- Impacto: Se entiende como las consecuencias ocasionadas por la materialización del riesgo. (DAFP 2018).
- Integridad: Propiedad de exactitud y completitud. (DAFP 2018).
- Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto. (DAFP 2022).
- 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. (DAFP 2022).
- 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: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. (DAFP 2022).
- 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).