DIRECCIÓN DE PLANEACIÓN

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

VIGENCIA 2025

Proceso Gestión Tecnológica

Enero 2025

Gobernación de Cundinamarca | EPC Empresas Públicas de Cundinamarca S.A. E.S.P. | pda Cundinamarca | #PrimeroEnAgua

Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, está orientado a una cultura de carácter preventivo que permita establecer las acciones para la reducción de la afectación en el caso de materialización, de igual maneraen el presente documento se desarrollará estrategias para el tratamiento, evaluación y monitoreo de los riesgos, con el propósito de no comprometer los objetivos demarcados por Empresas públicas de Cundinamarca.

Objetivo General

Definir y aplicar los lineamientos para el tratamiento de los riesgos de Seguridad de la Información, de tal manera que permita alcanzar los objetivos propuestos, la misión y visión institucional, alcanzando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Objetivos Específicos

- Dar cumplimiento con los requisitos legales y reglamentos aplicables.

- Gestionar el tratamiento de los riesgos de Seguridad de la Información.

Marco normativo

Documento CONPES 3854 de 2017 “Política Nacional de Seguridad Digital”

Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”

ISO 27001 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

Guía para la administración del riesgo y el diseño de controles en entidad públicas, Versión 6, noviembre de 2022, Departamento Administrativo de la Función Pública.

Demás normas o políticas aplicables o que modifiquen, adicionen o sustituyan las normas antes enunciadas.

Alcance

El presente documento establece la gestión de los riesgos de seguridad de la información con el fin de integrar los procesos, las buenas prácticas para la toma de decisiones y Para la elaboración del plan de tratamientos se tendrá en cuenta la Guía para la administración del riesgo y el diseño de controles en entidad públicas.

Marco Referencial

Política de administración de riesgos, cuyo propósito es establecer lineamientos acerca del tratamiento, manejo y seguimiento a los riesgos, los niveles de responsabilidad y las acciones frente a una posible materialización, con el fin de cumplir con los objetivos estratégicos. EPC (Empresas públicas de Cundinamarca) define su política de administración de riesgos tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión - MIPG, en el cual se articulan los riesgos de gestión, corrupción y seguridad de la información. Así mismo se acoge la metodología elaborada por el Departamento Administrativo de la Función Pública, secretaria de Transparencia de la Presidencia de la República y el Ministerio de Tecnología de la Información y Comunicaciones, quienes para el efecto elaboraron la Guía para la administración del Riesgo y el Diseño de Controles.

Desarrollo metodológico

Fase 1: Análisis de la información. En esta etapa se evaluarán los resultados de las entrevistas con cada uno de los procesos, del cual se desarrollarán las siguientes actividades:

- Revisión de riesgos.

- Valoración de riesgos.

Fase 2: Revisión y análisis de las acciones de tratamiento. En esta fase se realizarán las actividades que permitan la estructuración de las acciones de tratamiento.

- Determinar el nombre de la acción de tratamiento.

- Definición de las acciones de tratamiento relacionadas con cada riesgo.

- Definir los responsables de cada acción de tratamiento.

- Definir las fechas en las que se desarrollarán las acciones de tratamiento.

Fase 3: Consolidación de la matriz de riesgos: En esta fase se realizará la consolidación de la matriz de riesgos identificados por cada uno de los procesos, estará liderada por la Oficina Asesora de Planeación.

Fase 4: Ciclo de vida del tratamiento de riesgos: Realizar seguimiento a cada una de las acciones de tratamiento establecidas, basado en las fechas de cumplimiento, entregable y responsable.

Metodología - Plan de tratamiento

El plan de tratamiento de riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los **riesgos**, estructurada por tareas, responsable, fecha y entregables, atendiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Pr**ivacidad de la Información:**

Politica	Producto	Fecha Inicio	Fecha Fin
Realizar la valoración de los riesgos con respecto a Seguridad de la Información	Documentos de riesgos respecto a la seguridad de la información	1/04/2025	30/04/2025
Aprobación de la matriz de Riesgos y los planes de tratamiento	Acta de reunión y aprobación de matriz de riesgos	1/05/2025	30/05/2025
Publicar la Matriz de Riesgos	Enlace de publicación de la matriz de riesgos	1/06/2025	30/06/2025
Realizar Seguimiento a los Riesgos	Documento de seguimiento de los riesgos	1/07/2025	31/07/2025

Recursos

Las actividades señaladas anteriormente se realizarán con los profesionales con los que cuentan las áreas responsables, no se utilizarán recursos adicionales.

Medición del modelo de seguridad y privacidad de la información

La medición se realiza a través de indicadores que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la información