GOBERNACION DE CUNDINAMARCA

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

BOGOTA ENERO DE 2023

Contenido

1. OBJETIVO

Detallar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI de la Gobernación de Cundinamarca; de tal forma que se definen los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información en la Gobernación. De esta forma se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, que las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad.

2. ALCANCE

El plan de tratamiento de riesgos tiene alcance para los procesos implementados y soportados en el Documento Alcance del SGSI de la Gobernación de Cundinamarca, en concordancia con lo establecido en la norma ISO 27001:2022 para el Sistema de Gestión de Seguridad de la Información.

3.TERMINOS Y DEFINICIONES

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad, para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

SIGC (Isolucion): Es el sistema integrado de Gestión de la Gobernación de Cundinamarca, que permite armonizar los procesos en búsqueda de una gestión eficiente, eficaz y trasparente, con el fin de aumentar la satisfacción de los usuarios.

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

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información – SGSI - de la Gobernación de Cundinamarca, se busca prevenir los efectos no deseados, que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

5. MARCO REFERENCIAL

5.1. Política de administración de riesgos

La Gobernación de Cundinamarca, a través de su Sistema de Gestión de Seguridad de la Información, se orienta hacia una cultura de la gestión de riesgos de la Información, asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TICs, que contribuyen al desarrollo social y económico del Departamento, al desarrollo integral de los ciudadanos Cundinamarqueses y la mejora en su calidad de vida.

El objetivo de la gestión de los riesgos de Seguridad y Privacidad de la información, están establecidos en Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Gobernación, con el fin de dar continuidad a la gestión Departamental y asegurar el cumplimiento de los compromisos con los Cundinamarqueses.

El tratamiento de riesgos de Seguridad dela Información, es la respuesta establecida por la primera línea de defensa, es decir, el responsable del proceso, junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

• Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. La aceptación del riesgo puede ser una opción viable en la Gobernación, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles, y por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

• Reducir el riesgo: Se adoptan controles y lineamientos para reducir la probabilidad o el impacto del riesgo; por lo general conlleva a la implementación de controles. Deben seleccionarse controles

apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

• Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

• Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este con los proveedores informáticos. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

6 METODOLOGIA

El Plan de Tratamiento de Riesgos de Seguridad de la Información, contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)

Actividad	**Descripción**	**Responsable**	**Fecha inicial planificada**	**Fecha final planificada**
Adecuar y Aprobar el procedimiento de GESTIÓN DE ACTIVOS DE INFORMACIÓN TIC. *	Se definirán los controles a implementar a nivel de seguridad y privacidad y de mitigación del riesgo de Seguridad de la Información, mediante la adecuación de la Guía Gestión y Clasificación de Activos de Información TIC, la Matriz de Valoración de Riesgos de Activos de Información y la Guía Gestión de Riesgos Activos de Información TIC.	TIC – DDO - PLANEACION	10/01/2023	30/04/2023
Documentar y aprobar los roles y responsabilidades para la implementación del SGSI, acorde a lo establecido en	Se implementara lo establecido en la guía Roles y responsabilidades del Sistema de Gestión de Seguridad de la Información - SGSI el cual consiste en el desarrollo de las tareas	TIC – DDO (Isolucion) - PLANEACION	10/01/2023	30/04/2023

las Guías del Mintic. *	correspondientes a la implementación del SGSI.			
Jornadas de Capacitación a las entidades involucradas en el alcance del SGSI	Capacitación y creación de cultura institucional en Riesgos de Seguridad de la Información	TIC – PLANEACION - Isolucion	30/02/2023	31/12/2023
Levantamiento y/o valorización de los riesgos de información acorde a la nueva tipificación de riesgos. *	Se realizarán las actividades para la mejora del SGSI como la adecuación de políticas por dominio, procedimiento de gestión de incidentes y unificación de acuerdos de confidencialidad.	TIC, Función Pública y Gestión de Ingresos de la Sede central de la Gobernacion	30/06/2023	31/12/2023
Levantar y Aprobar la información documentada del proceso de seguridad de la información que conlleve a la mitigación de los riesgos de seguridad de la información.	Realizar el levantamiento de la respectiva documentación del proceso de seguridad de la información como (guías, procedimientos, políticas, planes y formatos) correspondientes al proceso.	TIC, Función Pública, Sec. General y Gestión de Ingresos de la Sede central de la Gobernación de Cundinamarca	25/01/2023	31/12/2023

6.1. PROGRAMACIÓN DE MONITOREO DE CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se programa el monitoreo de los controles definidos en cada uno de los riesgos de seguridad y privacidad de la Información, identificados con la sigla SGSI (Sistema de Gestión de Seguridad de la Información); de manera trimestral.

7. MARCO LEGAL

• Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

• Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

• Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

8. REQUISITOS TÉCNICOS

• Norma Técnica Colombiana NTC/ISO 27001:2022 Sistemas de gestión de la seguridad de la información.

• Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

9. DOCUMENTOS ASOCIADOS

- Gestión de Seguridad de la InformaciónA-GSI-GUI-003 Guía Gestión Riesgos activos información
- Gestión de Seguridad de la InformaciónA-GSI-FR-003 Matriz de gestión de riesgos de seguridad de la información
- Gestión de Seguridad de la InformaciónA-GSI-GUI-001 GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN v1
- Gestión de Seguridad de la InformaciónA-GSI-FR-002 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN v1

10. RESPONSABLE DEL DOCUMENTO

Secretaria de Tecnologías de Información y Comunicaciones – Dirección de Infraestructura Tecnológica, secretaria de la Función Pública – Dirección de Desarrollo Organizacional

Cordial saludo

YURY ALEXANDER RIVEROS
Gobernación de Cundinamarca
Secretaria de Tecnologías de la Información y las comunicaciones
Dirección de Infraestructura Tecnológica