Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Ministerio de Cultura

Contenido

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información establece el conjunto de actividades para crear condiciones de uso confiable en el entorno digital y físico de la información, fundamentado en las buenas prácticas de la Norma Técnica ISO 31000:2018, ISO 27001:2013 y en cumplimiento de la normativa establecida por el estado colombiano, CONPES 3854 de 2016, CONPES 3995 DE 2020, Modelo de Seguridad y Privacidad de MINTIC ,el decreto 1008 de 14 de junio 2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 5 2020 emitida por el DAFP.

En el plan se contemplan estrategias que reduzcan el impacto de afectación a los activos de información y permitan preservar la confidencialidad, integridad y disponibilidad de la información, adicional se busca desarrollar actividades para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos.

2.OBJETIVOS

OBJETIVO GENERAL

Establecer el plan de tratamiento de riesgos de seguridad de la información que permita mantener la integridad, confidencialidad y disponibilidad de la información mediante la gestión de riesgos asociados a la información de la Entidad.

OBJETIVOS ESPECÍFICOS

- Proteger y reducir el riesgo asociado a los activos de información.
- Identificar riesgos en cada uno de los procesos y subprocesos institucionales que afecten la triada de la información.
- Asignar los controles existentes para cada uno de los riesgos identificados que ayuden a la mitigación del riesgo
- Realizar seguimiento de los planes de manejo para el tratamiento de los riesgos identificados.

3.CONTEXTO INSTITUCIONAL

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Alta Dirección del Ministerio de Cultura se encuentra comprometida con la administración integral de riesgos, a través del fortalecimiento de directrices que permiten gestionar, evitar, prevenir, asumir, reducir, compartir o transferir los riesgos que pueden implicar efectos negativos en la Entidad, tanto como aquellos que permiten aprovechar, potenciar, operar y/o aumentar las oportunidades de mejorar la eficacia del Sistema Integrado de Gestión Institucional.

Así mismo, se gestionan de manera integral las amenazas externas y debilidades internas, los riesgos de calidad para los productos y servicios, los riesgos de seguridad de la información y los posibles actos que se deriven de los riesgos de corrupción, mediante el monitoreo periódico a la eficacia y efectividad de los controles establecidos por los procesos. El seguimiento a esta gestión es realizado por la Oficina de Control Interno y publicado conforme a los requerimientos legales vigentes para la toma decisiones por parte de la Alta Dirección.

En su compromiso con la promoción de los riesgos positivos, entendidos como oportunidades externas o fortalezas internas que permiten orientar y alinear los riesgos con los objetivos estratégicos y dar cumplimiento a la normatividad legal vigente; la Alta Dirección vela por la superación de sus capacidades internas en relación con el contexto interno y externo que afecta sus prioridades.

En concordancia con lo mencionado, se establecen las siguientes directrices:

- La Administración del Riesgo es gestionado basándose en el concepto de oportunidad, legalidad y como un asunto clave para el éxito de su planeación estratégica.

- La Administración del Riesgo considera como un factor de riesgo, todo aquello que afecte la calidad de los productos, servicios y trámites de la Entidad e impacta la satisfacción de los ciudadanos, usuarios y/o beneficiarios.

- La Administración del Riesgo para la entidad considera los efectos del incumplimiento de la legislación vigente y desarrollo jurisprudencial que puedan conllevar a detrimento patrimonial, multas, hallazgos de los entes de control, tutelas, fallos judiciales en contra y cualquier evento de daño antijurídico, de ética pública y compromiso ante la comunidad.

- La Alta Dirección determinará los recursos necesarios para la gestión del riesgo, propiciando espacios de participación de los colaboradores, un proceso permanente de comunicación, revisión, seguimiento y control a las acciones de mejora para el tratamiento de los riesgos.

- En la implementación de una nueva política cultural, así como en el diseño y/o desarrollo de nuevos productos y servicios se deberá tener en cuenta la metodología establecida en el P-OPL-013 Procedimiento de Administración del Riesgo, a fin de que el responsable del proceso actúe de manera preventiva, realizando la respectiva identificación, análisis, evaluación y establecimiento de controles que prevengan la materialización del riesgo o la potenciación de oportunidades.

- Para la identificación y tratamiento de los riesgos de seguridad de la información o riesgos digitales, se debe tomar como insumo los activos de información de cada proceso y su clasificación en términos de nivel de criticidad.

- Los riesgos transversales serán monitoreados y gestionados por los procesos que tienen en su propósito las cuestiones o eventos a mitigar o potenciar, sin embargo, por su carácter transversal los procesos afectados tendrán la oportunidad de manifestar sus consideraciones y opiniones en la construcción de los mapas, en la gestión de los controles, en el monitoreo y en el seguimiento.

- El monitoreo de los mapas de riesgos y la implementación de los controles se realizará por parte de los líderes de cada proceso y/o

proyecto, conforme el ciclo de control aprobado en el marco de este documento en su capítulo final.

- Se tendrá en cuenta para los Riesgos con nivel de riesgo residual diferente de bajo, la implementación de los planes de tratamiento a los riesgos, acorde con los lineamientos definidos por MINTIC.

4. DESARROLLO METODOLÓGICO

METODOLOGÍA

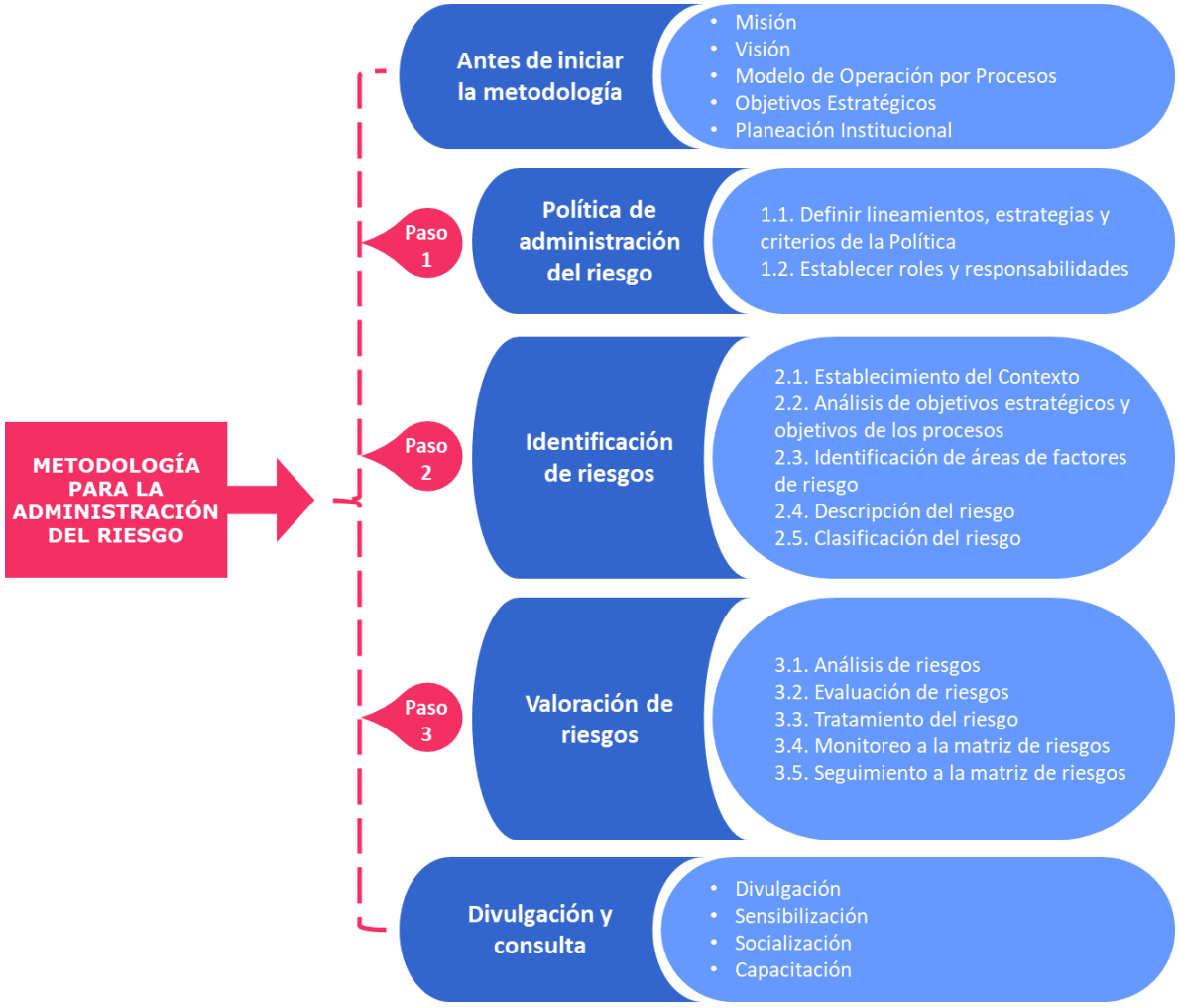

Ilustración 1 Gestión de riesgos, Fuente: Guía para la gestión de riesgos - SIGI del Ministerio de Cultura – G-OPL-019

ANÁLISIS DE INFORMACIÓN

El insumo para la identificación será el levantamiento, clasificación y actualización de activos de información y los resultados de la aplicación,

que se pueden encontrar en el botón de transparencia de la página web del Ministerio de Cultura de acuerdo con lo establecido en la Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones” y los decretos o resoluciones que la reglamentan.

IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

Se identifican las amenazas, vulnerabilidades, consecuencias y se determina la probabilidad e impacto que pueden llegar a afectar a uno o varios activos de información, interrumpiendo la operatividad institucional.

VALORACIÓN DE RIESGOS

La valoración del riesgo en seguridad de la información es un proceso fundamental, en donde se establecen los criterios para:

- Realizar valoración y aceptación de riesgos.
- Identificación de eventos que atenten contra la disponibilidad, confidencialidad y/o integridad de la información.
- Analizar los riesgos en términos de probabilidad e impacto y determinar su nivel.

Se busca establecer la probabilidad de ocurrencia y el impacto que tendrá la afectación del activo con el fin de estimar el riesgo inherente

TRATAMIENTO DE RIESGOS

El tratamiento del riesgo consiste en identificar y aplicar los controles adecuados, con el fin de mitigar la materialización del riesgo, evitando así los daños intrínsecos.

Los controles por implementar se deben basar a los propuestos en el Anexo A de la NTC-ISO-IEC 27001:2013.

MONITOREO DE RIESGOS

Para tal fin, cada responsable de proceso y subproceso debe realizar trimestralmente el respectivo monitoreo a los riesgos de seguridad de la información, en la herramienta dispuesta por la Oficina Asesora de Planeación. Igualmente, se debe realizar el respectivo seguimiento a la aplicación de planes de tratamiento del riesgo establecido, que para el efecto se pudo dejar como una acción correctiva o de mejora.

5.PLAN DE IMPLEMENTACIÓN

ACTIVIDADES	TAREAS	ENTREGABLES
Gestión Riesgos de Seguridad y Privacidad de la Información		
Actualización metodologías	Actualización de guía	Guía actualizada G-OPL-019
Identificación de riesgos	Identificar, analizar y evaluar los riesgos	Correo electrónico, Actas mesas de trabajo
	Revisión, validación y ajustes de riesgos.	
Aceptación de riesgos	Cargar riesgos identificados en ISOLUCION	ISOLUCION, módulo riesgos para cada uno de los procesos y subprocesos que identificaron riesgos.
	Flujo de aprobación del riesgo en ISOLUCION	
	Establecer el plan de manejo para el tratamiento de los riesgos.	
Seguimiento a planes de manejo	Revisión de la documentación y evidencias cargadas en los planes de manejo.	Correo electrónico, Actas mesas de trabajo
Evaluación de riesgos residuales.	Evaluar los controles implementados determinando la disminución de probabilidad e impacto.	Correo electrónico, Actas mesas de trabajo
Mejoramiento	Identificación de oportunidades de mejora conforme a los resultados de la evaluación del riesgo residual	Correo electrónico, Actas mesas de trabajo, ISOLUCION

6. REFERENCIAS

- Decreto 1078 del 26 de mayo del 2015 “Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones”
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- 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 (MinTIC)
- Guía de gestión del riesgo, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013
- Norma Técnica Colombiana NTC-ISO 31000:2011
- Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 5 2020.