Plan de Tratamiento de Riesgos de Seguridad de la Información para la CNSC

Marco contextual

La Comisión Nacional del Servicio Civil - CNSC ha desplegado durante las vigencias anteriores una estrategia de gestión de los riesgos siguiendo las recomendaciones del Departamento Administrativo de la Función Pública – DAFP y en el marco de las buenas prácticas contempladas en la norma técnica colombiana NTC/ISO 31000 versión 2009, y para ello cuenta con su documento orientador para aplicar de manera efectiva los conceptos de gestión denominado "***Guía de Implementación y Administración del Riesgo en la CNSC – G-SG-002***". Bajo estos conceptos se ha desarrollado el presente "***Plan de Tratamiento de Riesgos de Seguridad de la Información para la CNSC***".

Antecedentes

A mediados del año 2018, se logró que la Oficina Asesora de Planeación integrara en su guía metodológica de gestión de los riesgos, que se hiciera una revisión de dicha guía para incluir parámetros medición para facilitar la valoración de los riesgos y que además se incluyeran los conceptos de afectación del riesgos a la seguridad de la información, con el propósito que con este instrumento se unificaran los esfuerzos de los diversos procesos para identificar y valorar los riesgos y sus respectivas consecuencias de materialización y así mismo poder calificar la efectividad de los controles existentes para cada riesgo. Estas incluidas en la "Guía de Implementación y Administración del Riesgo en la CNSC – G-SG-002", permitieron que se hiciera una valoración más precisa de los riesgos identificados en la Comisión y de paso se asociaran con la Seguridad de la Información.

Otra consecuencia favorable de la actualización de este documento, fue la liberación de una nueva versión para el formato "***Mapa de Riesgos - F-SG-004*** v4" y la publicación oficial de los formatos "***Plan de Tratamiento de Riesgos - F-SG-014*** v1" y "***Gestión para la materialización de riesgos del Proceso*** - F-SG-015 v1".

Objetivo General del Plan

Implementar las actividades de control derivadas de las políticas de tratamiento para los riesgos identificados y valorados por cada uno de los procesos institucionales y hacer un seguimiento programado de las mismas, con el propósito de verificar su efectividad en el

control de cada uno de los riesgos que según la ***Guía de Implementación y Administración del Riesgo en la CNSC – G-SG-002***, ameritan la formulación de acciones para tratamiento de los mismos.

Alcance del Plan

Este plan pretende cubrir en la vigencia 2019, el proceso de publicación de las actividades de tratamiento de los riesgos, haciendo énfasis en aquellos que tienen afectación directa al Sistema de Gestión de Seguridad de la Información, hasta la valoración de la efectividad de las acciones emprendidas y efectividad de los controles propuestos para cada proceso para gestionar adecuadamente los riesgos calificados con valor **ALTO** o **EXTREMO**.

Como resultado del proceso de la valoración de los riesgos y sus controles, se han identificado un total de dieciséis (16) riesgos que ameritan acciones de tratamiento los cuales se presentan en la siguiente tabla:

RIESGOS VALORADOS QUE OBLIGAN ACCIONES DE TRATAMIENTO				
COD.	**DESCRIPCIÓN**	**VALOR RESIDUAL**	**POLÍTICA DE TRATAMIENTO**	**PROCESO INSTITUCIONAL**
R012	Errores en la información que se publica	**Alto**	Mitigar	Gestión de Comunicaciones
R014	Desactualización de la información publicada en el sitio web	**Alto**	Evitar	Gestión de Comunicaciones
R031	Incumplimiento en la concertación y evaluación de desempeño de los servidores de carrera administrativa	**Alto**	Mitigar	Talento Humano
R033	Perdida de información	**Extremo**	Mitigar	Talento Humano
R034	Pérdida de oportunidad para ejercer la defensa de La Entidad	**Alto**	Mitigar	Representación Judicial y Extrajudicial
R037	Ataques informáticos	**Alto**	Mitigar	Gestión de Recursos Tecnológicos
R038	Pérdida de información	**Alto**	Mitigar	Gestión de Recursos Tecnológicos
R042	Daño en equipos informáticos asignados a los funcionarios en los puestos de trabajo.	**Alto**	Mitigar	Gestión de Recursos Tecnológicos
R051	Inadecuado control de visitantes y/o contratistas.	**Alto**	Mitigar	Gestión de Recursos Tecnológicos
R054	Alteración o manipulación de la información y/o documentos oficiales	**Alto**	Mitigar	Gestión Documental
R055	Perdida de trazabilidad en el sistema	**Alto**	Mitigar	Gestión Documental
R056	Imputación de gastos al rubro presupuestal que no corresponde	**Alto**	Evitar	Gestión de Recursos Financieros
R059	Destinación de recursos de CNSC hacia actividades que no están planificadas y no se relacionan con su misión y con el desarrollo de las funciones institucionales.	**Alto**	Evitar	Gestión de Recursos Financieros

RIESGOS VALORADOS QUE OBLIGAN ACCIONES DE TRATAMIENTO				
COD.	**DESCRIPCIÓN**	**VALOR RESIDUAL**	**POLÍTICA DE TRATAMIENTO**	**PROCESO INSTITUCIONAL**
R073	Pérdida o Robo de Bienes (consumo - devolutivos)	**Alto**	Mitigar	Infraestructura
R075	Contaminación al medio ambiente	**Alto**	Mitigar	Infraestructura
R076	Perdida o fuga de información	**Extremo**	Mitigar	Infraestructura

Tabla 1. Riesgos que ameritan plan de tratamiento.

Entre dichos riesgos, se puede identificar que estos tiene algún grado de afectación a la seguridad de la información, razón por la cual el contenido del formato ***F-SG-014 - PLAN DE TRATAMIENTO DE RIESGOS***, se considera como el detalle desagradado de las acciones del presente plan.

Actividades del Plan.

Actividad / Tarea	Responsable	Fecha Inicio	Fecha Fin	Observaciones
Análisis de resultados de Valoración de riesgos y planes de tratamiento.	Gestores del SIG Gestor del SGSI	**06/01/2019**	**30/01/2019**	*Depende de la entrega de los resultados de las matrices de riesgos de los procesos actualizadas a 2018.*
Generación y Publicación del Plan de Tratamiento de Riesgos de Seguridad de la Información	Gestores del SIG Gestor del SGSI	**31/01/2019**	**04/02/2019**	*Depende de la entrega de los resultados de las matrices de riesgos de los procesos actualizadas a 2018.*
Programar actividades de seguimiento a las acciones contenidas en el plan detallado (Formato F-SG-014)	Gestores del SIG	**04/02/2019**	**01-03-2019**	*Corresponde a un documento concertado entre el SIG y los procesos involucrados*
Realizar el acompañamiento que sea explícitamente en la ejecución de las acciones del plan detallado	Gestor del SGSI	**01/03/2019**	**13/12/2019**	*Se atienden las solicitudes que se radiquen ante la OAI.*
Seguimiento de las acciones del Plan de Tratamiento de Riesgos de Seguridad de la Información.	Gestores del SIG Gestor del SGSI	**01/03/2019**	**13/12/2019**	*Actividad trimestral de acompañamiento a la OAP.*
Valoración del Plan de Tratamiento de Riesgos de Seguridad de la Información para la vigencia.	Gestores del SIG Gestor del SGSI	**13/01/2020**	**17/01/2020**	*Consolidación de los resultados suministrados por los procesos y consolidados por la OAP.*

Tabla 2. Plan de Tratamiento de Riesgos de Seguridad de la Información.