Integración de los Planes Institucionales y Estratégicos
al Plan de Acción Institucional

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

Vigencia 2020

Oficina Asesora de Planeación
Oficina Asesora de Informática

Versión 1
Enero, 2020

Tabla de contenido

1. Objetivo

Verificar la adecuada implementación y operación de las actividades de control derivadas de las políticas de tratamiento para los riesgos identificados y valorados por cada uno de los procesos institucionales, así como 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, especialmente para aquellos riesgos que tienen alguna afectación a la Seguridad de la Información.

2. Alcance

Este plan pretende cubrir en la vigencia 2020, desde el acompañamiento a las actividades de tratamiento de los riesgos identificadas por los líderes de los procesos institucionales, haciendo énfasis en aquellos que pueden generar algún tipo de afectación 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.

3. Alineación estratégica

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 las buenas prácticas incluidas en la norma técnica colombiana NTC/ISO 31000 versión 2009, y para ello cuenta con el documento orientador denominado “Guía de Implementación y Administración del Riesgo en la CNSC – G-SG-002”, que es usado para aplicar de manera efectiva, los conceptos de gestión del riesgo. Estas acciones buscan atender las necesidades de prevención que hacen parte de la estrategia denominada “***Mejoramiento de las Capacidades de Gestión Institucional***”, cuyo desarrollo apoya todos los objetivos estratégicos de orden misional de la Entidad. Bajo estos conceptos se ha desarrollado el presente “***Plan de Tratamiento de Riesgos de Seguridad de la Información para la CNSC***”.

4. Glosario

Concepto	Definición
Riesgo	Efecto de la incertidumbre en los objetivos (ISO 27000:2014 Numeral 2.68. Risk). Es toda posibilidad de ocurrencia de aquella situación que puede afectar el desarrollo normal de la entidad y el logro de sus objetivos.
Seguridad de la Información	Conjunto de técnicas y métodos encaminados a la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión (ISO 27000:2014 Numeral 2.33. Information security).

Tabla 1. Definiciones

5. Normatividad Aplicable

Normatividad	Descripción
Ley 1712 de 2014	Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Compilado en el Decreto Único Reglamentario 1081 de 2015 del Sector Presidencia de la República.
Decreto 612 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
NTC/ISO 27001 de 2013	Sistemas de gestión de la seguridad de la información. Requisitos
Riesgos de gestión, corrupción y seguridad digital. Versión 4 - Octubre de 2018	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 4 de Octubre de 2018.

Tabla 2. Normatividad aplicable

6. Desarrollo

Como resultado del proceso de la valoración de los riesgos y sus controles durante la vigencia 2019, han quedado de manera puntual doce (12) 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 pública	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

Riesgos Valorados que Obligan Acciones de Tratamiento				
Cod.	**Descripción**	**Valor Residual**	**Política de Tratamiento**	**Proceso Institucional**
R033	Pérdida de información	Extremo	Mitigar	Talento Humano
R034	Pérdida de oportunidad para ejercer la defensa de La Entidad	Alto	Mitigar	Representación Judicial y Extrajudicial
R042	Daño en equipos informáticos asignados a los funcionarios en los puestos de trabajo.	Alto	Mitigar	Gestión de Tecnologías de la Información
R054	Alteración o manipulación de la información y/o documentos oficiales	Alto	Mitigar	Gestión Documental
R055	Pérdida 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
R073	Pérdida o Robo de Bienes (consumo - devolutivos)	Alto	Mitigar	Infraestructura
R075	Contaminación al medio ambiente	Alto	Mitigar	Infraestructura

Entre dichos riesgos, se puede identificar que éstos, tienen 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*** que se ha consolidado para toda la Comisión, se puede considerar como el detalle de actuación del presente plan.

7. Actividades

Actividad	Producto	Responsable	Fecha Inicio	Fecha Fin
Análisis de resultados de Valoración de riesgos y planes de tratamiento.	Depende de la entrega de los resultados de las matrices de riesgos de los procesos actualizadas a 2019.	Enlaces del SIG Gestor del SGSI	**13/01/2020**	**28/02/2020**
Programar actividades de seguimiento a las acciones contenidas en el plan detallado (Formato F-SG-014)	Corresponde a un documento concertado entre el SIG y los procesos involucrados	Enlaces del SIG	**03/02/2020**	**28/02/2020**
Realizar el acompañamiento que sea explícitamente solicitado por los responsables de los procesos para la ejecución de las acciones del plan detallado	Se atienden las solicitudes que se radiquen ante la OAI.	Gestor del SGSI	**02/03/2020**	**18/12/2020**
Seguimiento de las acciones del Plan de Tratamiento de Riesgos de Seguridad de la Información.	Actividad cuatrimestral de acompañamiento a la OAP.	Enlaces del SIG Gestor del SGSI	**02/03/2020**	**18/12/2020**
Valoración del Plan de Tratamiento de Riesgos de Seguridad de la Información para la vigencia.	Consolidación de los resultados suministrados por los procesos y consolidados por la OAP.	Enlaces del SIG Gestor del SGSI	**07/01/2021**	**13/01/2021**

8. Anexos

Este documento tiene como anexos los formatos consolidados y publicados tanto en la Intranet como en el portal Web de la Comisión:

Mapa de Riesgos F-SG-004
Plan de Tratamiento de Riesgos F-SG-014

9. Control de cambios

Fecha	Cambio	Solicitada por
08/01/2020	Formulación del plan	Jefe de la Oficina Asesora de Planeación Jefe de la Oficina Asesora de Informática