CNSC
COMISIÓN NACIONAL DEL SERVICIO CIVIL
Igualdad, Mérito y Oportunidad

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 2021

Oficina Asesora de Planeación
Oficina Asesora de Informática

Versión 1
Diciembre, 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 2021, 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 y de aquellos riesgos que presenten algún caso de materialización en esta vigencia.

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 2018, 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 estratégica institucional 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 actualizado 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.

Concepto	Definición
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 nueve (9) riesgos que ameritan acciones de tratamiento, y además se reportó la materialización de siete (7) riesgos, los cuales se presentan en la siguiente tabla:

Cod.	Descripción	Valor Residual	Política de Tratamiento	Proceso Institucional
R-CM-003	Filtración de las pruebas de procesos de selección por mérito, antes de su aplicación a los aspirantes.	Alto	Mitigar	Concurso de Méritos
R-ED-001	Incumplimiento por parte de las entidades públicas de normatividad en materia de EDL.	Alto	Mitigar	Evaluación del Desempeño Laboral

Cod.	Descripción	Valor Residual	Política de Tratamiento	Proceso Institucional
R-TI-012	Daño en equipos informáticos asignados a los funcionarios en los puestos de trabajo.	Alto	Mitigar	Gestión de Tecnologías de la Información
R-GF-001	Imputación de gastos al rubro presupuestal que no corresponde.	Alto	Evitar	Gestión Financiera
R-GF-004	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 Financiera
R-IT-001	Pérdida o robo de bienes (consumo - devolutivos).	Alto	Mitigar	Infraestructura
R-IT-003	Contaminación al medio ambiente.	Alto	Mitigar	Infraestructura
R-RL-001	Pérdida de oportunidad para ejercer la defensa de La Entidad.	Alto	Mitigar	Representación Judicial y Extrajudicial
MATERIALIZADOS				
R-TI-001	Disminución de la oportunidad, eficiencia y efectividad en la prestación de los servicios TIC.	Medio	Mitigar	Gestión de Tecnologías de la Información
R-TI-005	Funcionalidad de las aplicaciones que no corresponde a lo esperado por el usuario.	Medio	Mitigar	Gestión de Tecnologías de la Información
R-TI-010	Instalación de software no autorizado o uso no autorizado de software valido por parte de cualquier colaborador de la Comisión.	Bajo	Mitigar	Gestión de Tecnologías de la Información
R-TI-014	Inadecuada gestión de las contraseñas.	Medio	Mitigar	Gestión de Tecnologías de la Información
R-TI-015	Descarga de aplicaciones, datos, imágenes o en general contenidos de internet sin control.	Bajo	Mitigar	Gestión de Tecnologías de la Información
R-TI-016	Uso de programas utilitarios o herramientas especializadas que cambien los controles establecidos.	Bajo	Mitigar	Gestión de Tecnologías de la Información
R-TI-017	Eventos o incidentes sin solución definitiva.	Medio	Mitigar	Gestión de Tecnologías de la Información

Tabla 3. Lista de Riesgos con Planes de Tratamiento y Riesgos Materializados que tuvieron tratamiento

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

A continuación, se presenta la relación de las actividades más relevantes que deben ser desarrolladas para que el plan de tratamiento de riesgos institucional y de seguridad de la información contengan la posibilidad de materialización de éstos.

No.	Actividad	Meta/ Producto	Responsable	Fecha Inicio	Fecha Fin
1	**Validar la completitud de los riesgos relacionados como resultado de la actualización del Análisis de riesgos y de las actividades de los planes de tratamiento propuestos.**	Matriz de riesgos actualizada Plan de tratamiento de riesgos revisado	Enlaces del SIG Gestor del SGSI Gestor del SIG	18-01-2021	26-02-2021
2	**Programar actividades de seguimiento a las acciones contenidas en el plan detallado (Formato F-SG-014).**	Cronograma de actividades de seguimiento del plan.	Enlaces del SIG	01-02-2021	26-02-2021
3	**Realizar jornadas de sensibilización para el adecuado reporte y consolidación de información de la Gestión de Riesgos, de la materialización y de las actividades de Tratamiento a los enlaces SIG.**	Listas de asistencia a la sensibilización (Trimestral)	Enlaces del SIG Gestor del SGSI Gestor del SIG	01-02-2021	26-11-2021
4	**Realizar el acompañamiento que sea explícitamente solicitado por los responsables de los procesos para la ejecución de las acciones del plan detallado.**	Actas de reunión para atender las solicitudes que se radiquen ante la OAI o en la OAP	Gestor del SGSI	01-02-2021	30-12-2021
5	**Seguimiento de las acciones del Plan de Tratamiento de Riesgos de Seguridad de la Información.**	Formato de seguimiento a planes institucionales (Trimestral)	Enlaces del SIG Gestor del SGSI Gestor del SIG	01-02-2021	26-11-2021
6	**Valoración del Plan de Tratamiento de Riesgos de Seguridad de la Información para la vigencia.**	Acta de reunión sobre resultados del último seguimiento al plan	Gestor del SGSI Gestor del SIG	10-01-2022	14-01-2022
7	**Atender ejercicios de evaluación o seguimiento según requerimientos internos**	Informe de Auditoría o seguimiento Planes de mejoramiento (si aplica)	Gestor del SGSI Gestor del SIG Involucrados en la Gestión de riesgos y tratamiento de riesgos	01-02-2021	30-12-2021

8. Anexos

Como soporte de los casos de planes de tratamiento involucrados y de la gestión de riesgos materializados, se adjunta un archivo que contiene tres formatos diligenciados a saber:

F-SG-004 Mapa de Riesgos
F-SG-014 Plan de Tratamiento de Riesgos
F- SG- 015 Materialización del Riesgo

Archivo adjunto:

- 2020_mapa-de-riesgos_v2_2020-10-27.xlsx

9. Control de cambios

Fecha	Cambio	Solicitada por
13/01/2020	Formulación del plan	**José Jorge Roca Martínez** Jefe Oficina Asesora de Planeación **Gustavo Adolfo Vélez Achury** Jefe Oficina Asesora de Informática
02/01/2021	Actualización del plan para la vigencia 2021	**José Jorge Roca Martínez** Jefe Oficina Asesora de Planeación **Gustavo Adolfo Vélez Achury** Jefe Oficina Asesora de Informática

Elaboró	Revisó	Aprobó
Nombre: Maribel Carolina González Moreno **Cargo:** Contratista Gestor del SIG **Dependencia:** Oficina Asesora de Planeación **Nombre:** Hugo Fernando Ramírez Ospina **Cargo:** Contratista Gestor del SGSI **Dependencia:** Oficina Asesora de Informática	**Nombre:** Maribel Carolina González Moreno **Cargo:** Contratista **Dependencia:** Oficina Asesora de Planeación	**Nombre:** José Jorge Roca Martínez **Cargo:** Jefe Oficina Asesora de Planeación **Dependencia:** Oficina Asesora de Planeación **Nombre:** Gustavo Adolfo Vélez Achury **Cargo:** Jefe Oficina Asesora de Informática **Dependencia:** Oficina Asesora de Informática