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 2022

Oficina Asesora de Planeación
Dirección de Tecnologías de la Información y las Comunicaciones

Versión 1
Enero, 2022

CNSC
COMISIÓN NACIONAL DEL SERVICIO CIVIL
Igualdad, Mérito y Oportunidad

Tabla de contenido

Tabla de contenido 1

1. Objetivo 2
2. Alcance 2
3. Alineación estratégica 2
4. Glosario 2
5. Normatividad Aplicable 3
6. Desarrollo 4
7. Actividades 5
8. Presupuesto (PAA) 8
9. Anexos 8
10. Control de cambios 9

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 identificada de forma explícita alguna afectación a la Seguridad de la Información.

2. Alcance

Este plan pretende cubrir en la vigencia 2022, 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 – SGSI, 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

Tabla 1. Definiciones

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

Concepto	Definición
	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).

5. Normatividad Aplicable

Tabla 2.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
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
Documento CONPES 3995, 01 de julio de 2020	Política nacional de confianza y seguridad digital
NTC/ISO 27001 de 2013	Sistemas de gestión de la seguridad de la información. Requisitos
Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020.

6. Desarrollo

Como resultado del proceso de la valoración de los riesgos y sus controles durante la vigencia 2021, han quedado de manera puntual nueve (9) riesgos que ameritan acciones de tratamiento, y además se reportó la materialización de tres (3) riesgos, los cuales se presentan en la siguiente tabla:

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

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
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-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 Física
R-IT-003	Contaminación al medio ambiente.	Alto	Mitigar	Infraestructura Física
MATERIALIZADOS				
R-TI-011	Ataques informáticos.	Bajo	Mitigar	Gestión de Tecnologías de la Información
R-TI-004	Caída del portal web y los servicios desplegados a través de dicho portal.	Medio	Mitigar	Gestión de Tecnologías de la Información
RC009	Alteración o manipulación de la información y/o documentos oficiales.	Bajo	Mitigar	Gestión Documental

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.

Tabla 4. Relación de actividades del plan de tratamiento de riesgos para la seguridad de la información en la vigencia 2022

Plan de Tratamiento de Riesgos con énfasis en Seguridad de la Información					Metas para seguimiento				
No.	**Actividad**	**Meta/ Producto**	**Responsable**	**Plazo de Ejecución**	**Trimestre I**	**Trimestre II**	**Trimestre III**	**Trimestre IV**	**Total**
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	01/02/2022 – 29/04/2022	Matriz institucional de riesgos actualizada	-	-	-	1 matriz de riesgos actualizada y publicada = 100%
2	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	Enlaces del SIG Gestor del SGSI Gestor del SIG	08/04/2022 08/08/2022	-	Lista de asistencia a sensibilización sobre riesgos y tratamiento de riesgos	-	Lista de asistencia a sensibilización sobre riesgos y tratamiento de riesgos	2 listas de asistencia a jornadas de sensibilización = 100%
3	Programar actividades de seguimiento a las acciones contenidas en el plan detallado (Formato F-SG-014).	Cronograma de actividades de seguimiento del plan de tratamiento de riesgos de seguridad de la información.	Enlaces del SIG	04/03/2022 – 16/12/2022	-	Cronograma de actividades de seguimiento a planes formulados	-	-	1 cronograma de seguimiento a los planes de tratamiento = 100%

Plan de Tratamiento de Riesgos con énfasis en Seguridad de la Información					Metas para seguimiento				
No.	**Actividad**	**Meta/ Producto**	**Responsable**	**Plazo de Ejecución**	**Trimestre I**	**Trimestre II**	**Trimestre III**	**Trimestre IV**	**Total**
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 DTIC o en la OAP	Gestor del SGSI	Por demanda	-	-	-	-	Atención del 100% de las solicitudes de acompañamiento recibidas.
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	04/03/2022 – 16/12/2022	Informe de avance del plan	Informe de avance del plan	Informe de avance del plan	Informe de avance del plan	4 informes de avance del plan = 100%
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	04/03/2022 – 16/12/2022	Evaluación al informe de avance	Evaluación al informe de avance	Evaluación al informe de avance	Evaluación al informe de avance	4 evaluaciones a los informes = 100%

8. Presupuesto (PAA)

Para la vigencia 2022, no se han dispuesto rubros específicos del presupuesto económico para la realización de las actividades formuladas en el plan.

Los colaboradores de planta o contratistas que ejercen los roles de Enlaces SIG, Gestor del SIG y Gestor del SGSI, incluyen las actividades de acompañamiento, ejecución y seguimiento del plan de tratamiento de riesgos, como parte de las tareas de apoyo a la gestión institucional y por tanto los costos que se derivan de estas actividades se distribuyen en los gastos de funcionamiento de la Entidad.

9. Anexos

Se adjunta el resultado de los seguimientos internos realizados al plan formulado para la vigencia 2021 y el mapa de riesgos con los reportes de los riesgos que tienen plan de tratamiento formulado y los reportes de los riesgos materializados

Archivo:

- Avance_Plan_TTO-Riesgos_Diciembre2021.pdf

- 2021_Riesgos_procesos_Junio_2021_Publicada.xls

10. 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
05/01/2022	Actualización del plan para la vigencia 2022	**José Jorge Roca Martínez** Jefe Oficina Asesora de Planeación **Hernán Darío Gutiérrez Casas** Director de Tecnologías de la Información y las Comunicaciones - DTIC

Elaboró	Revisó	Aprobó
Nombre: Hugo Fernando Ramírez Ospina **Cargo:** Contratista Gestor del SGSI **Dependencia:** Dirección de Tecnologías de la Información y las Comunicaciones – DTIC	**Nombre:** Nelsy Aracely Garzón Guzmán **Cargo:** Contratista Gestor del SIG **Dependencia:** Oficina Asesora de Planeación	**Nombre:** José Jorge Roca Martínez **Cargo:** Jefe Oficina Asesora de Planeación **Dependencia:** Oficina Asesora de Planeación **Nombre:** Hernán Darío Gutiérrez Casas **Cargo:** Director **Dependencia:** Dirección de Tecnologías de la Información y las Comunicaciones - DTIC