



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

Plan de Implementación y Operación del Sistema de Gestión de Seguridad de la Información y del Modelo de Seguridad y Privacidad de la Información para la CNSC

Vigencia 2020

Oficina Asesora de Informática

Versión 1
Enero, 2020

Tabla de contenido

1. Objetivo	2
2. Alcance.....	2
3. Alineación estratégica.....	2
4. Glosario	2
5. Normatividad Aplicable	3
6. Desarrollo	4
6.1 Antecedentes.....	4
6.2 Direccionamiento de las Actividades del Plan.....	6
7. Actividades	6
8. Anexos	7
9. Control de cambios.....	8

1. Objetivo

Continuar con la implementación y operación del Subsistema de Gestión de Seguridad de la Información en la Comisión Nacional del Servicio Civil – CNSC, siguiendo los lineamientos de la Norma Técnica Colombiana NCT/ISO 27001 versión 2013 para Sistemas de Gestión de la Seguridad de la Información, y las buenas prácticas que, en materia de gestión administrativa, gestión del riesgo, operación de tecnología y seguridad informática se encuentren disponibles y sean aplicables en la Entidad.

2. Alcance

Este plan pretende cubrir en la vigencia 2020, el despliegue de los elementos necesarios para adelantar conjuntamente con otros sistemas de gestión del SIG tareas transversales del ciclo PHVA referentes a políticas, gestión de recursos, gestión documental, gestión operativa de los procesos, procedimientos de valoración, evaluación y seguimiento, y medidas de revisión por la dirección, que incluya la identificación, valoración y tratamiento de los riesgos identificados en los procesos, así como desplegar y operar los controles identificados y adoptados mediante la Declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información.

3. Alineación estratégica

Entendiendo que la Comisión Nacional del Servicio Civil - CNSC anualmente hace una revisión general a su plan Estratégico para el cuatrienio 2019 – 2022, en donde se incluye la estrategia “**Mejoramiento de las capacidades de gestión institucional**”, que apoya y contribuye directamente con el desarrollo y cumplimiento de todos los objetivos estratégicos de orden misional que al interior de la Comisión han sido adoptados, y tomando como base los resultados de dicha revisión, se ha desarrollado el presente “**Plan Implementación y Operación del Sistema de Gestión de Seguridad de la Información y del Modelo de Seguridad y Privacidad de la Información para la CNSC**”.

4. Glosario

Concepto	Definición
MSPI	Recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información, formulado por el Ministerio de las Tecnologías de la Información y Comunicación del Gobierno Colombiano.
Seguridad de la Información	Conjunto de técnicas y métodos encaminados a la preservación de la confidencialidad, integridad y disponibilidad de la información en

Concepto	Definición
	cualquiera de sus estados, medios de almacenamiento y/o difusión (ISO 27000:2014 Numeral 2.33. Information security).
SGSI	Un Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. (ISO 27000:2014 Numeral 3.2.1. Descripción y Principios).

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.
Ley 1955 de 2019	Por la cual se expide el Plan Nacional de Desarrollo 2018 -2022. " Pacto por Colombia, Pacto por la equidad". Artículo 147. Transformación Digital Pública, Artículo 148. Gobierno Digital como Política de Gestión y Desempeño Institucional. Artículos 147 y 148.
Ley 1960 de 2019	Por el cual se modifican la Ley 909 de 2004, el Decreto-ley 1567 de 1998 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 1499 de 2017	Por medio del cual se modifica el Decreto número 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
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
Documento CONPES 3854 de 2016	Política nacional de seguridad digital.
Documento CONPES 3975 de 2019	Política Nacional de Transformación Digital e Inteligencia Artificial.
Manual de Gobierno Digital - Abril 2019 de 2019	Implementación de la Política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2).
NTC/ISO 27001 de 2013	Sistemas de gestión de la seguridad de la información. Requisitos

Tabla 2. Normatividad aplicable

6. Desarrollo

6.1 Antecedentes.

Además de la implementación de controles y contramedidas de seguridad informática como el esquema de seguridad perimetral conformado por un dispositivo de balanceo de las comunicaciones entrantes y salientes de la Entidad, un dispositivo de corta-fuegos (firewall) para la contención y mitigación de posibles ataques informáticos, el monitoreo de tráfico de red, la renovación de las licencias del programa de antivirus para contrarrestar posibles apariciones y propagación de malware al interior de la Entidad, así como la gestión de incidentes de seguridad de la información detectados automáticamente o reportados por usuarios y la revisión del comportamiento de los sistemas de información publicados para la ciudadanía y otras partes interesadas, durante la vigencia de 2019, se avanzó en la implementación y formalización de actividades relevantes para la operación del SGSI así:

- Se adoptó formalmente la Declaración de Aplicabilidad, respecto a los controles de operación del Sistema de Gestión de Seguridad de la Información.
- Se identificaron las necesidades de intercambio y obligatoriedad de suministro de información, por lo cual se formalizó la guía para la gestión de los grupos de interés y las autoridades en la CNSC (G-SG-SI-002).
- Se llevó a cabo una revisión y fortalecimiento de la metodología de gestión de los riesgos en la Entidad, publicándose la quinta versión de la guía de implementación y administración del riesgo (G-SG-002).
- Se emitió un documento de sensibilización y concienciación para que todos los colaboradores de la Comisión (de planta o contratistas) conozcan las responsabilidades y deberes que se deben tener respecto a la Seguridad de la Información en la Comisión, y para ello, se publicó el Manual de Responsabilidades (M-SG-SI-001).
- Se formalizó y aplicó el Procedimiento Gestión de Activos de la Información - P-SG-006 y se adelantó un levantamiento de inventarios de estos activos por proceso.
- Se hizo un esfuerzo por revisar la documentación de la Oficina Asesora de Informática, para aportar al mejor desarrollo operacional del SGSI, generando nuevos documentos o versiones de los siguientes instrumentos:
 - Procedimiento Desarrollo de Software (P-TI-001)
 - Procedimiento Gestión de Cambios (P-TI-005)
 - Procedimiento Gestión de Usuarios de TI (P-TI-006)
 - Procedimiento Para la prestación de servicios TI (P-TI-007)
 - Procedimiento Gestionar la Plataforma de TI (P-TI-008)
 - Procedimiento Gestión de la capacidad de TI (P-TI-009)
 - Guía Para el uso adecuado de internet en la CNSC (G-TI-002)
 - Guía Estratégica para la gestión de los servicios de TI (G-TI-003)
 - Guía para la Gestión de los Grupos de Interés y las Autoridades en la CNSC (G-TI-004)

- Instructivo Para el uso adecuado de los recursos tecnológicos (I-TI-002)
- Instructivo Protección de la información digital - Herramienta de cifrado (I-TI-003)
- Instructivo para el uso de dispositivos móviles y medios de almacenamiento extraíbles (I-TI-004)
- Instructivo para conexión segura de trabajo remoto por VPN (I-TI-005)
- Instructivo Para gestionar las vulnerabilidades técnicas (I-TI-006)
- Protocolo Uso interno de la mensajería instantánea (PR-TI-002)

Respecto a los 114 controles indicados en el Anexo A de la Norma Técnica Colombiana NTC/ISO 27001, se puede decir que: Se tienen plenamente implementados 45 controles del Anexo A, equivalentes al 39,47 por ciento; se tienen con baja implementación 49 controles del Anexo A, equivalentes al 42,98 por ciento; Se encuentran en fase de implementación 14 controles del Anexo A, equivalentes al 12,28 por ciento y se encuentran en fase de diseño 6 controles del Anexo A, equivalentes al 5,26 por ciento.

También se puede afirmar que, con corte al 31 de diciembre de 2019, se están trabajando todos los controles del Anexo A de la NTC/ISO 27001 versión 2013 y dichos controles presentan algún grado de avance.

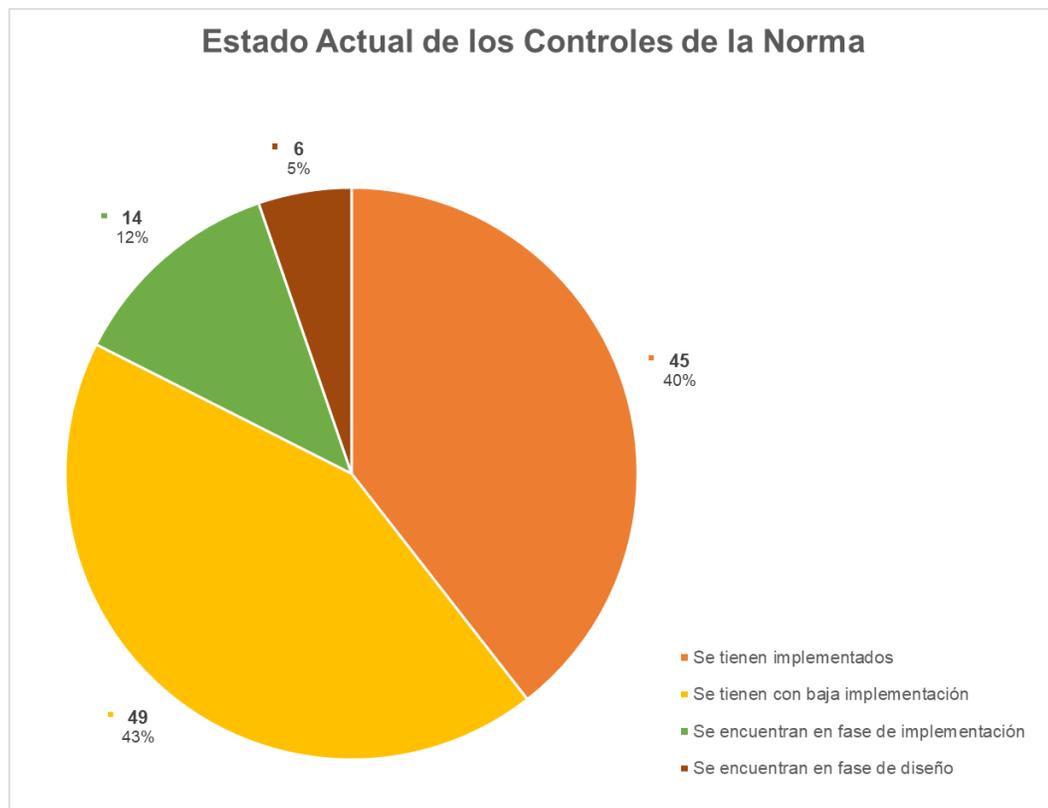


Ilustración 1. Nivel de implementación de los controles del Anexo A, con corte a diciembre de 2019

6.2 *Direccionamiento de las Actividades del Plan.*

El enfoque principal que se dará al MSPI fundamentado en la implementación del SGSI para la vigencia 2020, será el de afianzamiento, interiorización y despliegue de los controles adoptados en la vigencia anterior, así como dar continuidad a la formalización de la información documentada requerida, tanto por los procesos misionales, como por el proceso de gestión de tecnologías de la información, con el propósito de hacer partícipes a todos los colaboradores de la Entidad en lo referente a la Seguridad de la Información.

7. Actividades

Actividad / Tarea	Productos	Responsable	Fecha Inicio	Fecha Fin
Elaborar una estrategia combinada para divulgar, promover y aplicar en toda la Entidad los documentos y controles del SGSI que la OAI ha desplegado.	Documento de definición de la estrategia de divulgación. <i>Nota: Se requiere un apoyo permanente para que la información y los controles que se han adoptado operen adecuadamente en todos los procesos institucionales.</i>	Gestor del SGSI Jefe de la OAI Comunicaciones	20/01/2020	20/11/2020
Realizar seguimiento a los controles administrativos del SGSI	Incluye siete (7) tareas específicas: a) Revisión de las Políticas de Direccionamiento Estratégico b) Apoyar la ejecución de procedimiento de gestión de los activos c) Diseño de la guía de clasificación, etiquetado y marcación de la información d) Colaborar con un análisis de responsabilidades por proceso e) Recomendar	Gestor del SGSI Gestor del SIG	13/01/2020	26/06/2020



CNSC

COMISIÓN NACIONAL
DEL SERVICIO CIVIL

Igualdad, Mérito y Oportunidad

Actividad / Tarea	Productos	Responsable	Fecha Inicio	Fecha Fin
	controles para los proyectos internos f) Seguimiento y verificación de contratos con proveedores g) Formalizar el procedimiento de Tratamiento de Datos Personales.			
Colaborar con la revisión de la gestión contrato de vigilancia y el desarrollo de la seguridad física de la CNSC	Actas de reunión. <i>Nota: Se planean reuniones bimestrales.</i>	Gestor del SGSI Gestor del SIG Director de DAC	13/01/2020	18/12/2020
Plan de Recuperación ante desastres de TI (DRP-TI)	Documento del DRP.	Gestor del SGSI Jefe de la OAI	13/01/2020	18/12/2020
Realizar seguimiento a los controles tecnológicos del SGSI	Incluye tareas específicas de documentación de actividades, seguimiento y revisión: a) Documentación mediante instructivos. b) Seguimiento a mantenimientos operativos. c) Verificación de resultados de consolas de trabajo.	Gestor del SGSI Líderes de grupos funcionales de la OAI	13/01/2020	18/12/2020

8. Anexos

Se anexa a este documento el detalla desagregado de actividades propuestas para su adecuado despliegue.

Plan de trabajo detallado para el MSPI – SGSI.
Archivo: Actividades_Plan_MSPI-SGSI_2020.xlsx



9. Control de cambios

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