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

Marco contextual

Entendiendo que la Comisión Nacional del Servicio Civil - CNSC anualmente hace una revisión general a su plan Estratégico la el cuatrienio 2019 – 2022, en donde se incluye el objetivo estratégico "***Fortalecer la imagen y confianza institucional con el fin de ser el referente de la meritocracia en Colombia***" en el desarrollo de sus metas estratégicas requiere que al interior de la Comisión, sea desarrollado un "***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***".

Antecedentes

Se valoran los esfuerzos de la Oficina Asesora Informática que durante los años 2014 a 2016 adelantó frente a la implementación de controles y contramedidas de seguridad informática como fueron la adquisición de un esquema de seguridad perimetral conformado por un dispositivo de balanceado de las comunicaciones entrantes y salientes de la Entidad, un dispositivo de corta-fuegos (firewall) para la contención y mitigación de posibles ataques informáticos y la renovación de las licencias del programa de antivirus para contrarrestar posibles apariciones y propagación de malware al interior de la Entidad.

A finales del año 2017, se aplicó el instrumente de Auto-evaluación del estado del Modelo de Seguridad y Privacidad de la Información – MSPI, suministrado por el Ministerio de las Tecnologías de la Información – MinTIC que arrojó entre otros los siguientes resultados:

Modelo de MSPI – Ciclo PHVA

Etapa	Logro
Planificación (P)	9%
Implementación (H)	1%
Evaluación del desempeño (V)	0%
Mejora continua (A)	0%

Componente de Ciberseguridad según el NIST

Componente	Logro
Identificar	9%
Detectar	8%
Responder	6%
Recuperar	27%
Proteger	2%

Niveles de Implementación del SGSI según ISO 27001:2013

Control	Logro
A.5 Políticas de la Seguridad de la Información	20%
A.6 Organización de la Seguridad de la Información	4%
A.7 Seguridad de los Recursos Humanos	13%
A.8 Gestión de Activos	6%
A.9 Control de Acceso	39%
A.10 Criptografía	10%
A.11 Seguridad Física y del Entorno	14%
A.12 Seguridad de las Operaciones	37%
A.13 Seguridad de las Comunicaciones	55%
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	4%
A.15 Relaciones con los proveedores	0%
A.16 Gestión de Incidentes de Seguridad de la Información	31%
A.17 Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio	10%
A.18 Cumplimiento	7,5%

Tomando como base estos resultados el 19 de septiembre de 2017, se generó la resolución 2017200058225 que adoptó para la CNSC la política de Seguridad de la Información, y definió su alcance al interior de la Entidad y sus objetivos primordiales.

Durante la vigencia de 2018, se avanzó en la implementación con las siguientes actividades relevantes:

- Se publicó el Manual de Políticas de Direccionamiento Estratégico (M-SG-SI-002).
- Se identificaron las necesidades y expectativas de la Comisión frente al Sistema de Gestión de Seguridad de la Información y se plasmó su resultado en documento conocido como la Guía de Identificación de partes interesadas, necesidades y expectativas (G-SG-SI-001).
- Se llevó a cabo una revisión y fortalecimiento de la metodología de gestión de los riesgos en la Entidad para que dicho instrumento sea de fácil aplicación y control en la Comisión y a su vez incluya los conceptos de Seguridad de la Información con un eje transversal a la Organización. Se publicó la cuarta versión de la guía de implementación y administración del riesgo (G-SG-002) y se adoptaron los formatos Mapa de Riesgos (F-SG-004), Plan de Tratamiento de Riesgos (F-SG-014), Materialización de Riesgos F-SG-015 y Juicio de expertos para la Valoración de Riesgos (F-SG-016) que desarrollan su debida aplicación.
- 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 han formalizado los procedimientos de Gestión de Incidentes de Seguridad de la Información (P-SG-SI-001) y Gestión de Cambios (P-TI-005), y los documentos de Estándares y Lineamientos para Desarrollo de Software (G-TI-001) y de Protocolo para el Control de Ingreso al Centro de Cómputo (PR-TI-001) que marcan el inicio de acciones concretas complementarias a las actividades de seguridad informática que la Oficina Asesora de Informática ya venía realizando.

Tomando como referencia el avance de los diferentes elementos del SGSI, basados en la Norma Técnica Colombiana NTC/ISO 27001 en su versión 213, se evidencian avances en el ciclo PHVA así:

Etapa	Logro
Planificación (P)	33%
Implementación (H)	28%
Evaluación del desempeño (V)	25%
Mejora continua (A)	14%

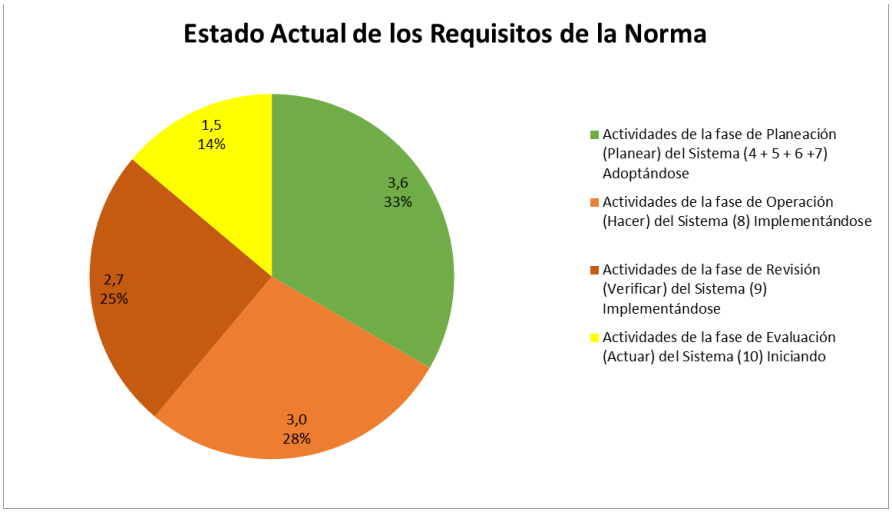

Ilustración 1. Cumplimiento de Actividades del Ciclo PHVA en el Año 2.018

Respecto a los 114 controles indicados en el Anexo A de la Norma Técnica Colombiana NTC/ISO 27001, se puede decir que: Se tienen implementados 11 controles del Anexo A, equivalentes al 9,65 por ciento. Se tienen con baja implementación 49 controles del Anexo A, equivalentes al 42,98 por ciento; se encuentran en fase de implementación 24 controles del Anexo A, equivalentes al 21,05 por ciento; se encuentran en fase de diseño 18 controles del Anexo A, equivalentes al 15,79 por ciento y NO se tienen implementados 12 controles del Anexo A, equivalentes al 10,53 por ciento.

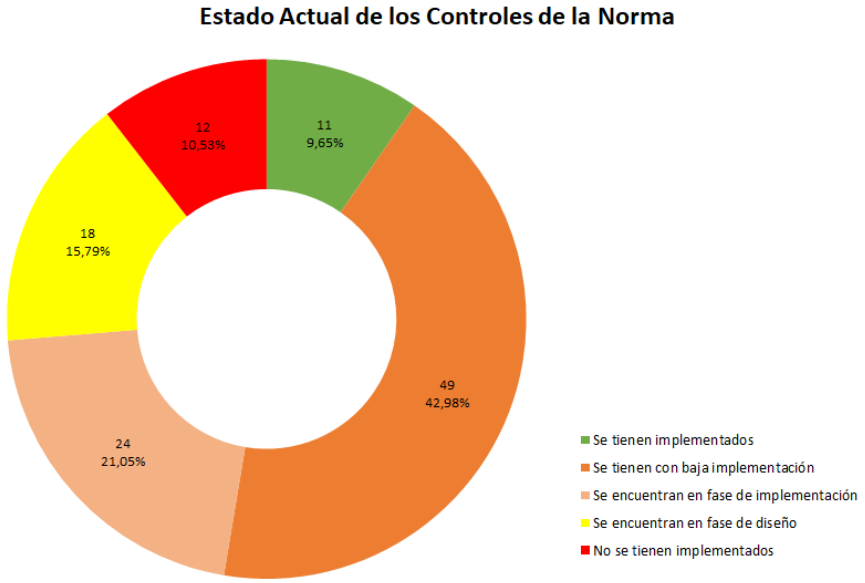

Ilustración 2. Nivel de implementación de los controles del Anexo A con corte a Noviembre de 2018

Objetivo General del Plan

Implementar el 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, Sistemas de Gestión de la Seguridad de la Información. Requisitos, 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.

Alcance del Plan

Este plan pretende cubrir en la vigencia 2019, 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, hasta que se pueda generar la Declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información en propiedad.

Actividades del Plan.

Actividad / Tarea	Responsable	Fecha Inicio	Fecha Fin	Observaciones
Análisis de resultados de Valoración de Riesgos y Planes de Tratamiento.	Gestor del SGSI	**26/11/2018**	**31/01/2019**	Actividad del plan 2018 no ejecutada. Depende de la entrega de los resultados de las matrices de riesgos de los procesos actualizadas a 2018.
Generación y Publicación de la DDA	Gestor del SGSI	**31/01/2019**	**22/02/2019**	Actividad del plan 2018 no ejecutada. Depende de la entrega de los resultados de las matrices de riesgos de los procesos actualizadas a 2018.
Divulgación de la DDA	Gestor del SGSI Jefe de la OAI Comunicaciones	**21/01/2019**	**1/03/2019**	Actividad del plan 2018 no ejecutada. Depende de la aceptación de la terminación de la Publicación de la DDA.
Coordinar Acciones Transversales del SGSI		**4/02/2019**	**29/03/2019**	
- Solicitud de información y acciones del SGSI relacionadas con Talento Humano	Gestor del SGSI Jefe de la OAI	4/02/2019	8/02/2019	Proceso: Talento Humano
- Solicitud de información y acciones del SGSI relacionadas	Gestor del SGSI Jefe de la OAI	18/02/2019	22/02/2019	Proceso: Infraestructura

con Infraestructura física y vigilancia				
- Solicitud de información y acciones del SGSI relacionadas con Gestión Documental	Gestor del SGSI Jefe de la OAI	4/03/2019	8/03/2019	Proceso: Gestión Documental
- Solicitud de información y acciones del SGSI relacionadas con Comunicaciones Institucionales	Gestor del SGSI Jefe de la OAI	4/02/2019	15/02/2019	Proceso: Gestión de Comunicaciones
- Solicitar a OCI incluir en el proceso de Evaluación y Seguimiento y en el plan de auditorías aspectos del SGSI	Gestor del SGSI Jefe de la OAI	4/03/2019	8/03/2019	Proceso: Control Interno y Disciplinario
Colaborar con la implementación del procedimiento de Gestión de Activos de Información	Gestor del SGSI	**18/02/2019**	**26/04/2019**	Actividad del plan 2018 no ejecutada.
Definir los mecanismos para la Gestión de Capacidad de TI	Gestor del SGSI Líder Infraestructura Arquitecto TI Jefe de la OAI	**4/02/2019**	**29/03/2019**	
Coordinar las actividades de Gestión de las Vulnerabilidades Técnicas	Gestor del SGSI Líder Infraestructura Jefe de la OAI	**1/04/2019**	**31/05/2019**	
Colaborar con la formalización documental de las actividades de TI (*)	Gestor del SGSI	**10/12/2018**	**22/11/2019**	Requiere la colaboración de los líderes de grupos funcionales de la OAI para revisión, ajuste y adopción.
Coordinar las actividades para generar la propuesta del DRP de TI que incluya elementos de Seguridad de la Información	Gestor del SGSI Líder Infraestructura Arquitecto TI Jefe de la OAI	**8/04/2019**	**31/05/2019**	Depende de los resultados del análisis de riesgos, de las necesidades expresadas por la Alta Dirección, de la revisión de los ANS y del presupuesto asignado.
Colaborar con la implementación de los controles del Anexo A que sean aplicables según la DDA y con aquellos que se requieren como buena práctica.	Gestor del SGSI Líder Infraestructura Jefe de la OAI	**17/06/2019**	**22/11/2019**	Depende de la aceptación de la terminación de la Publicación de la DDA. Se requiere colaboración de los líderes de grupos funcionales de la OAI.