Tabla de contenido

1. Objetivo

Ejecutar las actividades que permitan gestionar la seguridad de la información acorde con las necesidades de la CNSC, cumpliendo con el direccionamiento del Ministerio de las Tecnologías de la Información y las Comunicaciones y las buenas prácticas del mercado tecnológico para que los activos estratégicos y los servicios ofrecidos por la CNSC mantengan los niveles requeridos de confidencialidad, integridad y disponibilidad.

2. Alcance

Este es un proceso cíclico, que inicia con la revisión de los resultados alcanzados en la vigencia anterior y la evaluación del autodiagnóstico sobre el sistema de gestión, pasando por actividades cotidianas de revisión, monitoreo y acompañamiento, la realización de actividades específicas de control hasta consolidar los resultados y medir los avances de la gestión para la vigencia que concluye.

3. Diccionario Conceptual

Activo de Información: Un activo de información es cualquier recurso (físico, lógico o humano) que pueda contener o procesar información relevante para la Entidad.

Amenaza: Es toda aquella acción o situación que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. El origen de las amenazas suele ser externo o ajeno al control de la Entidad.

Ciberseguridad: Conjunto de medidas de “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.

Incidente: Causa una interrupción o afectación en el servicio. Interrupción no planificada de un servicio, reducción en la calidad de un servicio o un evento que aún no ha tenido impacto en el servicio para el cliente.

MSPI: El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información.

PETI: Sigla usada para referirse al Plan Estratégico de Tecnologías de la Información de la Entidad.

Seguridad de la Información: Es el 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*).

Seguridad informática: Es una disciplina tecnológica que se encarga de proteger la integridad y la privacidad de la información contenida o gestionada mediante sistemas informáticos.

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*).

Vulnerabilidad: Es el evento o situación que una persona, sistema u objeto puede sufrir frente a peligros inminentes, sean ellos desastres naturales, desigualdades económicas, políticas, sociales, tecnológicas o culturales. El origen de las vulnerabilidades suele ser interno y en la potestad de gestión por parte de la Entidad.

4. Normativa Aplicable

Ley 1273 de 2009 (05-01-2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1581 de 2012 (17-10-2012). Por la cual se dictan disposiciones generales para la protección de datos personales. "Ley de Protección de Datos Personales"

Ley 1712 de 2014 (06-03-2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 2108 de 2021 (29-07-2021). "Ley de Internet como servicio público esencial y universal" o por medio de la cual se modifica la Ley 1341 de 2009 y se dictan otras disposiciones.

Decreto 103 de 2015 (20-01-2015). Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1008 de 2018 (14-06-2018). 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Política de Gobierno Digital.

Directiva Presidencial 03 de 2021 (15-03-2021). Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Resolución MinTIC 500 de 2021 (10-03-2021). 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.

Manual de Gobierno Digital (abril 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).

Documento CONPES 3995 de 2020 (01-07-2020). Política nacional de confianza y seguridad digital.

Resolución Interna 20171200058225 del 19-09-2017, "Por la cual se actualiza la Política General de Seguridad y Manejo de la Información de la Comisión Nacional del Servicio Civil".

NTC/ISO 27001:2013 Sistemas de Gestión de Seguridad de la Información. Requisitos.

5. Políticas de Operación

Los lineamientos de la gestión de la seguridad de la información deben ajustarse a las necesidades y expectativas de los procesos misionales de la CNSC y se deben concertar junto con la Alta Dirección, el proceso de planeación y el proceso de gestión de tecnologías de la información a fin de mantener armonía e independencia en la ejecución de los planes y actividades propuestas.

El direccionamiento político y estratégico de la seguridad de la información en la Entidad se rige por las buenas prácticas y estándares internacionales en materia de seguridad de la información (familia de estándares ISO 27000) y por las guías del MSPI emitido por el MinTIC.

Los resultados de las evaluaciones y autoevaluaciones que se adelanten se deben medir tomando como base las evidencias ciertas y disponibles que evidencie o recopile el evaluador.

Este procedimiento no describe la forma de desplegar u operar el Sistema de Gestión de Seguridad de la Información - SGSI, solamente describe actividades específicas de la forma de administrar la seguridad de la información en la CNSC.

6. Desarrollo

Paso	Descripción	Responsable	Punto de Control	Registro
1.	Validar los resultados del autodiagnóstico del SGSI de la vigencia anterior. Se tiene como insumo el resultado del ejercicio de verificación de los resultados de la gestión de la seguridad de la información en la vigencia anterior, para identificar las brechas y oportunidades de mejora, así como la preservación de las actividades que han presentado buenos resultados.	Gestor del SGSI	-	-
2.	Revisar los lineamientos estratégicos institucionales actualizados. Se deben consultar las actualizaciones que se hayan realizado al Plan Estratégico Institucional - PEI, así como los resultados y avances de los proyectos y planes institucionales (PETI, Gestión de Riesgos, Tratamiento de Riesgos) para validar la pertinencia del alcance y los objetivos propuestos para el SGSI.	Gestor del SGSI	-	-
3.	Verificar las condiciones del contexto de ciberseguridad aplicables. Este ejercicio consiste en hacer una validación y actualización del contexto general del SGSI y de la Ciberseguridad de la Entidad teniendo en cuenta las partes interesadas, los controles existentes, las vulnerabilidades técnicas y su manejo, las amenazas y agentes de amenaza identificados, los riesgos actuales y nuevos y los activos de información o activos estratégicos, con el propósito de validar el panorama general de la seguridad de la información y las expectativas agregadas.	Gestor del SGSI	-	-
4.	Formular Plan MSPI para la vigencia. Teniendo en cuenta los insumos anteriores se procede a la formulación del Plan de trabajo para la operación y mantenimiento del MSPI y del SGSI para la siguiente vigencia, identificando las actividades más relevantes que son requeridas, los plazos de ejecución y	Gestor del SGSI	X	Plan MSPI-SGSI nueva vigencia

Paso	Descripción	Responsable	Punto de Control	Registro
	los recursos necesarios para alcanzarlas.			
5.	Validar alineación con el SIG. Al recibir el plan propuesto, se tiene en cuenta la respectiva alineación con el PEI y con el direccionamiento del SIG para la vigencia, así como las recomendaciones y orientaciones recibidas en la revisión por la Alta Dirección de los subsistemas.	Gestores del SIG	-	-
6.	¿Plan alineado? Se valida que el plan se ajuste en forma y contenido a los estándares de la CNSC. En caso negativo **sigue a 7.** Emitir instrucciones de ajuste. En caso afirmativo **sigue a 8.** Iniciar actividades del plan.	Gestores del SIG	-	-
7.	Emitir instrucciones de ajuste. De acuerdo con las evidencias encontradas, se deben proponer las mejoras o correcciones o ajustes que deben incluirse en el plan del MSPI para articularse con los otros subsistemas del SIG.	Gestores del SIG	-	-
8.	Iniciar actividades del plan. Se empiezan a ejecutar las diferentes acciones y tareas necesarias para cumplir los objetivos y metas propuestas en el plan del MSPI-SGSI para la vigencia.	Gestor del SGSI	-	-
9.	Iniciar actividades cíclicas de revisión y monitoreo. Bajo esta actividad se agrupan tareas rutinarias que se adelantan para mejorar y/o mantener los niveles adecuados de seguridad y ciberseguridad en la Entidad. Estas tareas incluyen la revisión diaria de las consolas de gestión del dispositivo de seguridad perimetral (FW), la consola de gestión del antivirus (Cylance Protect and Optics), de gestión de la plataforma (Zabbix). La revisión noticias de los centros autorizados de información sobre seguridad informática y ciberseguridad (CSIRT gobierno, NIST, OWASP, Tenable)	Gestor del SGSI	-	-
10.	Sensibilizar a los colaboradores de la CNSC. Elaborar o solicitar colaboración al proceso de Comunicaciones Institucionales para informar sobre alertas de seguridad, vulnerabilidades o	Gestor del SGSI	-	-

Paso	Descripción	Responsable	Punto de Control	Registro
	resumen de casos internos atendidos.			
11.	Notificar eventos o necesidades específicas sobre seguridad de la información. En cumplimiento del compromiso expuesto en el manual de responsabilidad del SGSI M-SG-SI-001, todos los colaboradores deben reportar tan pronto como sea posible, a través de los canales apropiados los eventos que puedan alterar la seguridad de la información, de los cuales conozca o sea testigo, así mismo, deben observar y reportar cualquier debilidad de los controles de seguridad de la información que sea observada o sospechada en los sistemas o servicios de la Comisión.	Usuario Final (Colaboradores de la CNSC)	-	-
12.	Acompañar la gestión de activos de información. En los plazos fijados en el plan del MSPI-SGSI se deben realizar las sesiones de acompañamiento y asesoría a los Enlaces del SIG de los diversos procesos institucionales para revisar y actualizar los inventarios parciales de activos de información.	Gestor del SGSI	-	-
13.	Acompañar la gestión de riesgos de la Entidad. En los plazos fijados en el plan del MSPI-SGSI se deben realizar las sesiones de acompañamiento y asesoría a los Enlaces del SIG de los diversos procesos institucionales para revisar y actualizar los mapas de riesgos.	Gestor del SGSI	-	-
14.	Asesorar a los colaboradores de la Entidad sobre seguridad de la información. Cuando sea pertinente presentar a los Directivos de los procesos institucionales alternativas para mejorar o implementar controles adicionales para los riesgos del proceso en búsqueda de proteger la confidencialidad, integridad y disponibilidad de la información. Asistir o acompañar a los líderes de los procesos institucionales en las actividades que requieran conceptos de seguridad de la información.	Gestor del SGSI	-	-
15.	Atender la gestión de incidentes de seguridad	Gestor del	-	-

Paso	Descripción	Responsable	Punto de Control	Registro
	de la información. En los casos que sea pertinentes, se debe activar el procedimiento institucional de gestión de incidentes de seguridad de la información que se reporten o se evidencien, para detectar, contener, erradicar y eliminar las causas que han dado lugar al incidente.	SGSI		
16.	Preparar informes y aplicar autodiagnóstico SGSI. Como conclusión de la gestión de las actividades del Plan y los resultados de las actividades rutinarias de la Gestión de la Seguridad de la Información Institucional. Los productos, resultados y documentos elaborados se deben valorar en la herramienta de autoevaluación dispuesta por el MinTIC para este plan.	Gestor del SGSI	X	Informes de la Gestión.
17.	Validar resultados de la gestión. En el ejercicio de la consolidación de los resultados de los subsistemas que hacen parte del SIG se verifican los resultados e informes de la gestión.	Gestores del SIG	-	-
18.	Presentar resultados a la Dirección. Los datos más relevantes y el nivel de cumplimiento de las actividades y objetivos de los subsistemas son presentados para una revisión detallada por la Dirección.	Gestores del SIG	-	-
19.	Remitir resultados y direccionamiento al SGSI. Las conclusiones y directrices de la Alta Dirección que resulten de la revisión adelantada serán comunicada a los líderes y gestores de los subsistemas, como un insumo para la revisión y formulación de la nueva versión de los planes aplicables a cada uno.	Gestores del SIG	-	-
20.	Incorporar necesidades y expectativas. Las recomendaciones emitidas por la Alta Dirección, las novedades presentadas en el mercado tecnológico, los resultados del PETI, así como las necesidades y expectativas formuladas desde los procesos institucionales se deben considerar para iniciar el nuevo ciclo de administración de la seguridad de la información.	Gestor del SGSI	-	-

7. Control de Modificaciones

Versión	Fecha de Vigencia	Modificación Realizada	Solicitada por
1.0	26-11-2021	Versión inicial del procedimiento	Director de Tecnologías de la Información y las Comunicaciones

Elaboró	Revisó	Aprobó
Nombre: Hugo Fernando Ramírez Ospina **Cargo:** Contratista – Gestor del SGSI **Dependencia:** Dirección de Tecnologías de la Información y las Comunicaciones.	**Nombre:** Karol Marcela Cuervo Cuervo **Cargo**: Profesional Especializado **Dependencia:** Oficina Asesora de Planeación **Nombre:** Nelsy Aracely Garzón Guzmán **Cargo**: Contratista **Dependencia:** Oficina Asesora de Planeación	**Nombre:** Hernán Darío Gutiérrez Casas **Cargo**: Jefe de la Dirección de Tecnologías de la Información y las Comunicaciones. **Dependencia:** Dirección de Tecnologías de la Información y las Comunicaciones.