Tipo de Informe	Preliminar		Definitivo	X	**Fecha de Emisión del Informe**	28	07	2022

1. INFORMACIÓN GENERAL

Proceso (s) Auditado (s):	Gestión de Tecnologías de la Información y las Comunicaciones
Actividad (es) auditada (s):	A. Direccionamiento estratégico de las tecnologías de la información B. Gestionar las soluciones basadas en software C. Prestar servicios de tecnologías de la información D. Gestionar los cambios de TI E. Gestionar la seguridad de la información
Dependencia:	Dirección de Tecnología de la Información y las Comunicaciones
Líder del Proceso / Jefe(s) Dependencia(s):	Hernán Darío Gutiérrez - Dirección de Tecnología de la Información y las Comunicaciones
Objetivo de la Auditoría:	Revisar las actividades establecidas en el proceso de Gestión de Tecnologías de la Información y las Comunicaciones para la definición y puesta de controles asociados a la gestión, incluyendo la seguridad de la información, así como su aplicación en proyectos de implementación y desarrollo de software.
Objetivos Específicos:	1. Verificar la planeación y definición del proyecto de TI (OnBase), desde el punto de vista funcional. 2. Verificar la ejecución y aplicación de los procedimientos, cambios de TI en elementos, recursos y/o servicios del ambiente de producción de los aplicativos de la CNSC. 3. Verificar el estado de avance en la implementación del Modelo de Seguridad y Privacidad de la Información.
Marco Normativo:	NTC - ISO 27001:2013 Ley de Transparencia y Acceso a la Información Pública, Ley 1712 de 2014 Resolución 1519 de 2020 Ley 1581 de 2012, Ley de Protección de Datos Personales
Alcance:	La auditoría se realizó desde la definición de la necesidad de implementación del Sistema de Gestión Documental, puesta en funcionamiento, aplicación de seguridad, cambios y verificación de manejo de incidentes, para el proyecto de OnBase. Para los demás elementos de la auditoría se tuvo en cuenta los registros del periodo comprendido entre el 01 de julio de 2021 y el 07 de julio de 2022.

Fecha Reunión de Apertura			**Vigencia Auditada**	2022
20	05	2022		

Auditor Líder	**Auditor (es) de Apoyo**
YANETH MONTOYA GARCÍA	WILLIAM LEONIDAS LARA PALACIOS

2. SITUACIONES DETECTADAS DURANTE EL PROCESO DE AUDITORÍA

2.1. Resumen de la auditoría

De acuerdo con el plan de auditoría propuesto, se desarrolló la auditoría a través de mesas de trabajo virtuales, revisión documental y reuniones presenciales.

Dado que algunos documentos de referencia en el Sistema de Gestión de Calidad y en el Sistema de Seguridad de la Información fueron emitidos durante los últimos 3 meses, y que además hubo acciones recientes que se consideraron importantes para la auditoría, se extendió el alcance de la auditoría para la evaluación de los registros, de la fecha inicialmente prevista que correspondía al 20 de mayo de 2022, hasta el 07 de julio de 2022.

En este documento se describen los principales aspectos encontrados durante la auditoría que representan un hallazgo, una observación o una oportunidad de mejora, y sobre los cuales también se generan recomendaciones.

El presente informe se ha dividido en las siguientes secciones, de acuerdo con las actividades del proceso y el alcance definido para esta auditoría:

Al final del informe se encuentra la relación de los hallazgos para que se genere el plan de mejoramiento frente a cada uno, sin embargo, se recomienda revisar en detalle todo el documento, debido a que se plantean a lo largo del mismo diferentes observaciones que, de no ser tenidas en cuenta, podrían llegar a convertirse en hallazgos ó en la materialización de un riesgo.

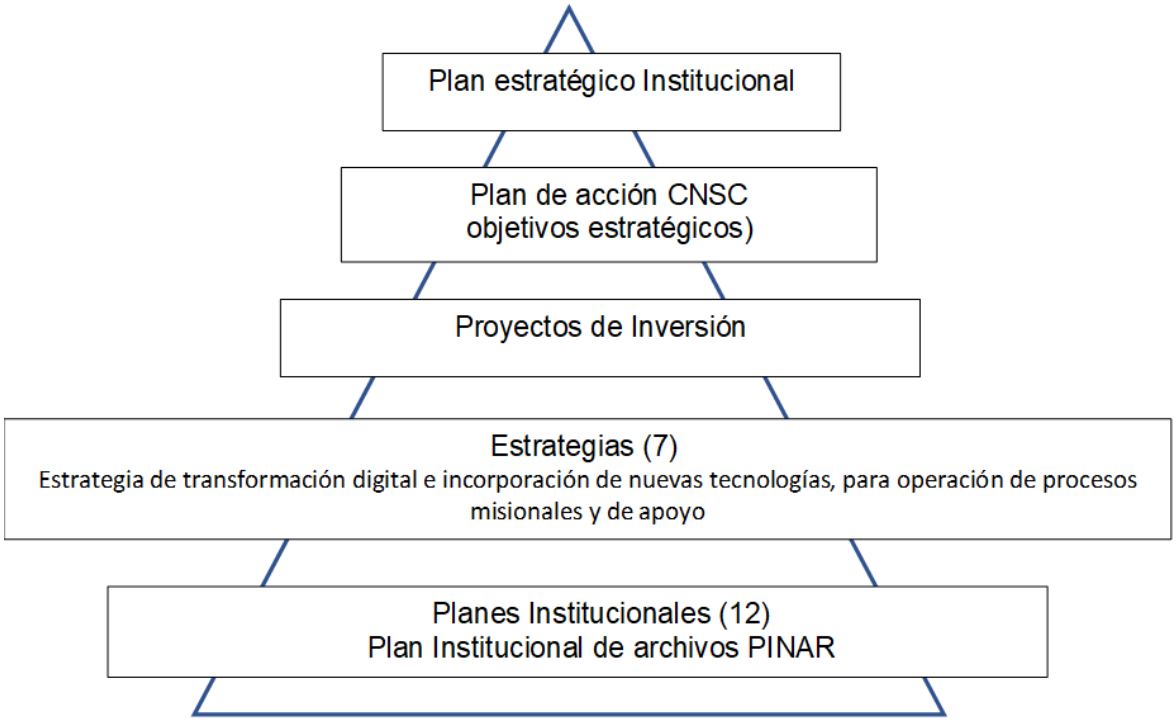
A. Direccionamiento estratégico de las tecnologías de la información

CARACTERIZACIÓN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN – TICS Versión: 4.0 Fecha: 26/11/2021 Código: C-TI-001

Se realizó la revisión a cada una de las actividades que establece la caracterización del proceso, como sigue:

- **Direccionamiento estratégico de las tecnologías de la información**

Se observó que existe una adecuada interrelación entre lo que se define como objetivo del proceso de Gestión de tecnologías de la información, con la planeación estratégica planteada por la CNSC, en su plan estratégico institucional (ver criterio 5), y en el plan de acción, (ver criterio 3), lo que permite establecer las acciones y decisiones que apuntan al cumplimiento de los objetivos estratégicos. Esto junto con los demás aspectos de la planeación que se evidenciaron, se muestran en la siguiente gráfica:



Se evidenció que se cuenta con el proyecto de inversión denominado FORTALECIMIENTO DE LA CAPACIDAD DE GESTIÓN INSTITUCIONAL DE LA CNSC-COMISIÓN NACIONAL, (ver criterio número 4). Que sirve como marco de inversión para el logro de tres (3) objetivos, y 4 productos o entregables que son:

- Sistemas de información,

- Servicios de información,
- Implementación de los sistemas de buenas prácticas de seguridad Política digital de MinTic, el Modelo de Privacidad y Seguridad de la Información, la NTC ISO 27001,
- Servicios tecnológicos y documentación requerida para la planeación de TI.

Continuando con la revisión de todo el direccionamiento estratégico, se revisó el Plan estratégico de las tecnologías de la información (PETI) (ver criterio 1), desde donde se sustentó la necesidad de implementar un sistema de gestión de documentos electrónicos de archivo SGDEA y 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 Versión 1 enero 2022. 2019, desde donde se efectuó el diagnóstico y el plan de implementación del modelo de las buenas prácticas de seguridad de la información definidas por MInTic (gobierno digital y el modelo de seguridad y privacidad de la información) y la norma NTC:ISO27001:2013.

En la desagregación de la planeación se revisó el Plan Institucional de Archivos - PINAR 2019 - 2022, donde se evidencian los aspectos críticos y riesgos, a partir de los cuales se definió la necesidad de formular un proyecto de SGDEA para optimizar los procesos y trámites de la entidad que se desarrollan en cumplimiento de las funciones asignadas, asegurando la legalidad, integridad, confiabilidad y usabilidad de la información que se recibe, produce y gestiona a través de diversos sistemas de información.

Se cuenta con el diagnóstico efectuado a la gestión documental, que identifica los metros lineales que se han generado para los archivos de gestión y central, el cual se encuentra publicado en Documentos del proyecto / Diagnóstico. Adicional se evidencia la ficha de proyecto que permite identificar el alcance, objetivos y riesgos del proceso entre otros dando Ficha del Proyecto OnBase respuesta a lo establecido en los criterios 8, 9 y 13.

A partir de la necesidad manifiesta de contar con una solución para dar respuesta a las debilidades que en materia de gestión documental se presentaban en la CNSC, se celebró el contrato 489 de 2020, con la empresa GIGA COLOMBIA S.A.S, adjudicado mediante resolución No 11022 DE 202006-11-2020 cuyo objeto consistió en adquirir e implementar el componente de software, como parte de un sistema de información que soporte el modelo corporativo de gestión documental en la Comisión Nacional del Servicio Civil -CNSC con la empresa se efectuó el respectivo proceso de contratación y que buscaba un nuevo software de gestión documental.

Se evidenció también la celebración del contrato de prestación de servicios No. 086 de 2022, cuyo objeto es: prestar servicios en modalidad de bolsa de horas para mantenimiento y desarrollos adicionales del gestor documental OnBase y adquisición de licencias para ampliación del cupo actual, y de acuerdo con el crecimiento de la planta que aumento de 400 a 600 usuarios, se revisó el número de licencias inicialmente asignadas. Licencias por suscripción o renta: Concurrent Client –10 licencias Workflow Concurrent Client SL –20 licencias Workwiew Concurrent Client SL –3 licencias.

De acuerdo con los antecedentes antes mencionados, se revisó en mesa de trabajo los objetivos y requerimientos que se establecieron para el proyecto OnBase:

Se evidenció que la metadata con la que OnBase permite generar la producción documental interna y externa, se estructuró con base en los grupos de gestión documental según las tablas de retención documental (TRD), y otra serie de propiedades que se diligencian o que automáticamente asigna el propio sistema. Dicha producción documental se gestiona a través de flujos de trabajo establecidos y estandarizados de acuerdo con el asunto y la data o propiedades asignadas, que permiten; ejecutar

tareas de manera automática, conocer al momento de la producción su avance y cuando se quiera consultar la existencia de alguna(s) comunicación(es) emitida(s), con algunas de las propiedades o data relacionada, y contar con información suficiente para conocer las acciones que se ejecutaron durante el trámite de la dicha comunicación o documento.

Se evidenció la forma como se establecen los permisos, roles y su segmentación en OnBase para consulta, modificación, borrado y/o eliminación de documentos, que se asigna a cada usuario que a través de la combinación de perfiles (administrador del sistema, administrador funcional, radicador entre otros), y privilegios (ver, crear, modificar entre otros), que está clasificado en grupos de usuario.

A continuación, se pudo evidenciar alguno de los requerimientos y mejoras adicionales logrados con la implementación del programa OnBase, como son; parametrización de actividades sin necesidad de conocimiento especializado de programación, balanceo de cargas o distribución de tareas, autenticidad de las comunicaciones mediante firma digital, tecnologías para migración de información ante cambios de tecnologías, estandarización y automatización de trámites, interoperabilidad con otros sistemas, la generación de reportes y por último para destacar el cumplimiento por parte de los documentos de atributos de ley que lo hacen convertirse en documentos con valor probatorio.

Se evidenció también las mejoras logradas con la implementación de OnBase en cuanto a simplificación, estandarización y automatización de los trámites y administración de toda la información de la entidad, como son los procesos de solicitud de traslado de docentes, integración con SIMO, solicitud de certificados y ventanilla única para PQRSF, entre otras.

B. Gestionar las soluciones basadas en software

Procedimiento DESARROLLO DE SISTEMAS DE INFORMACIÓN
P-TI-005 Versión: 6.0

Para esta sección de la auditoría se solicitó acceso en modo consulta al repositorio de GitLab, con el fin de verificar el documento de requerimiento (funcional y técnico) de la solución informática OnBase y verificar el control de las versiones de la solución OnBase en GitLab de código fuente y documentación técnica del proyecto.

No se encontró ninguna información sobre el proyecto OnBase en el repositorio. Según lo informado por la Dirección de Tecnologías de la Información y las Comunicaciones, en adelante DTIC, el repositorio de GitLab se está utilizando como repositorio de código fuente de los desarrollos internos y sobre OnBase no se tiene, dado que de este software se adquirieron licencias de uso a perpetuidad, más no se adquirió el código fuente, y la documentación técnica, así como la documentación de usuario final, se encuentra en el OneDrive de los ingenieros asociados al proyecto.

Observación: se recomienda definir la forma en que se organizará la documentación de los desarrollos o ajustes asociados a software de terceros, dado que OneDrive es un repositorio de carácter personal y se puede perder el control sobre esa información.

C. Prestar servicios de tecnologías de la información

Procedimiento GESTIONAR LA PRESTACIÓN DE SERVICIOS DE TI
P-TI-004 Versión 5.0

Se efectuó mesa de trabajo el miércoles, 29 de junio de 2022, 3:00 p.m.- 4:00 p.m., con representantes del proceso de Gestión de tecnologías de la información y las comunicaciones, quienes mostraron el manejo del programa de mesa de servicios GLPI, donde se gestionan los requerimientos que son solicitados, los cuales son identificados por tipo y en función de esa clasificación se evidenció la asignación de tiempos, y por ende el nivel de acuerdo de nivel de servicio, (ANS)

Observación: para tener acceso a la información de los tickets, la DTIC, otorgó a los auditores de la OCI, el rol de "Super-Admin", lo cual le permite a los mismos realizar cualquier tipo de cambio en la información. Si bien se tuvo acceso a la información, es riesgoso entregar ese tipo de privilegios. Por lo anterior, se recomienda generar un rol que permita a los auditores solamente visualizar la información.

Se efectuó una muestra aleatoria para corroborar la asignación de ANS, su tiempo de cumplimiento y acuerdo de nivel de servicio:

ID	fecha apertura	Descripción Solicitud	Fecha de solución	Fecha de cierre	Observación
98032	21/06/2022 9:19	Solicito su ayuda para ejecutar los scripts del archivo adjunto en el servidor TANIMUKA-BD, con el fin de solucionar varios casos del aplicativo EDL-APP.	24/06/2022 16:57	28/06/2022 8:37	No entra al KDB Se obtiene respuesta 5 del solicitante
98197	23/06/2022 21:03	Petición de Radicado 2022RE102216 Radicado de respuesta 2022RS061301	24/06/2022 7:50	27/06/2022 16:04	Se evidencia traza de respuesta al peticionario
97965	17/06/2022 10:08	Tiene relación con 97955	22/06/2022 16:43	23/06/2022 13:51	
97955	17/06/2022 7:58	Creación de usuario	17/06/2022 7:58	3/08/2022 7:58	
97782	14/06/2022 10:46	Desactivación de Orfeo y On base (97782)	14/06/2022 13:45	15/06/2022 14:00	
97756	14/06/2022 9:04	Reporte final de inscritos P.S. DIAN No. 2238 de 2021	14/06/2022 16:10	15/06/2022 14:00	
98034	21/06/2022 9:44	Ajuste rol aprobación	21/06/2022 15:44		En curso y por fuera del ANS
97596	9/06/2022 9:15	CREACION DE LA CUENTA DE ONBASE (97596)	9/06/2022 10:56	14/06/2022 8:58	ANS 6 horas (vencida)
97544	8/06/2022 13:56	Creación de ORFEO Y ONBASE	14/06/2022 9:18	9/06/2022 10:56	Vencida mayor a 6 h
98111	22/06/2022 13:16	CREACION DE LA CUENTA DE ONBASE (98111)	22/06/2022 16:52	23/06/2022 10:16	
97300	2/06/2022 17:55	Reporte Opec 4.0 superintendencia nacional de salud	2/06/2022 18:03	9/06/2022 17:00	ANS 36 horas

97333	3/06/2022 11:20	Reporte total de inscritos al Proceso de Selección DIAN No. 2238 de 2021	3/06/2022 12:28	21/06/2022 11:20	ANS 30 horas
97250	2/06/2022 10:03	Desactivación de Mesa de servicios	9/06/2022 9:52	09-06-2022 10:17	No tiene ANS
97100	27/05/2022 15:19	PARAMETRIZACION USUARIO BNLE 4.0	30/05/2022 12:24	2/06/2022 15:19	ANS 36 horas
97112	27/05/2022 17:23	chami1 (simo) - update tabla usuario_base	31/05/2022 0:23	1/06/2022 9:27	ANS 30 horas
97008	25/05/2022 17:19	CAMBIAR TIEMPOS REQUISITOS MINIMOS	26/05/2022 10:36	26/05/2022 10:36	ANS 30 horas
96788	20/05/2022 16:38	SOLICITUD REPORTE NOVEDADES REGISTRADAS BNLE 4.0	23/05/2022 15:23	7/07/2022 16:38	ANS 30 horas
96540	16/05/2022 9:17	SOLICITUD (desactivar usuario)	23/05/2022 15:35	23/05/2022 14:06	mayor al ANS
96389	11/05/2022 15:18	Solicitud reasignación radicado 2022RE078248	12/05/2022 15:25	16/05/2022 12:18	ANS 24 horas

De la muestra correspondiente a 20 tickets, se pudo evidenciar que 4 tickets tienen la fecha de respuesta superior a la fecha de solución, superando de esa manera el tiempo parametrizado y asignado para el acuerdo de nivel de servicio /ANS, un análisis más a fondo de las razones que impactaron el cumplimiento del ANS, su tipología, los inconvenientes al usuario, y a la seguridad de la información, permitirá concluir acerca de la gestión de la mesa de servicio y catálogo, tarea que debe ser abordada en la siguiente auditoría.

Así mismo, se pudo evidenciar que, para los tickets analizados y cerrados, no se incluyó algún dato o lección aprendida en la base de conocimientos con las que cuente el programa GLPI. De la misma manera, en la siguiente auditoría se debe incluir como objetivo.

D. Gestionar los cambios de TI

Procedimiento GESTIÓN DE CAMBIOS DE TI
P-TI-002 Versión: 3.0

Se recibió por parte del responsable de tecnología la base de datos de los cambios efectuados, de donde se extrajo, un caso específicamente para onBase. Caso 93196.

El caso se resume en que se solicitaba ajuste servicio de consulta estado radicados de entrada, y el cual fue gestionado de acuerdo con el procedimiento correspondiente. Se evidencia en el acta f-sg-009 acta-de-reunion-23-02-2022.docx., que no está relacionado el caso. Como recomendación se deja la necesidad de fortalecer el control de primera línea, por parte de quienes elaboración y revisaron el acta y de segunda línea, por arte de quienes aprueban. Se pudo observar que el acta no se encuentra firmada.

Hallazgo 1:
Con respecto a la revisión de información asociada al sistema OnBase, no se encontró documentación que permitiera evidenciar la trazabilidad en los cambios efectuados a dicho sistema. Se revisó en el repositorio de documentación técnica GitLab y en los tickets de GLPI, pero no se evidenciaron

archivos que den cuenta de los ajustes en las configuraciones, parametrizaciones y demás que se han hecho al mencionado sistema.

E. Gestionar la seguridad de la información

Procedimiento ADMINISTRAR LA SEGURIDAD DE LA INFORMACIÓN
P-TI-001 Versión: 2.0

Se evidencia en el documento **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** Versión 1 Enero 2022 donde se establece la planeación para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, atendiendo de esta forma lo indicado en la Política de Gobierno Digital, establecida por el MinTIC.

El resultado de la evaluación efectuada con corte a 20/12/2021, del Modelo de Privacidad y Seguridad de la Información y NTC ISO 27001 Anexo A, arrojo un resultado del 98%

El ejercicio de autodiagnóstico efectuado para el cumplimiento de la Política de Gobierno Digital, con corte a junio del 2021, arrojó un acumulado de 88%, para los 8 propósitos planteados por MinTic:

- Fortalecimiento de la Arquitectura Empresarial y de la Gestión de TI (85,7%)
- Fortalecimiento de la Seguridad y Privacidad de la Información (91,9%)
- Uso y apropiación de los Servicios Ciudadanos Digitales (55,0%)
- Servicios Digitales de Confianza y Calidad (100%)
- Procesos seguros y eficientes (74,7%)
- Toma de decisiones basadas en datos (88,9%)
- Empoderamiento de los ciudadanos mediante un Estado abierto (95,7%)
- Impulso en el desarrollo de territorios y ciudades inteligentes (100%)

Controles administrativos

Se realizó una revisión a la declaración de aplicabilidad de los controles administrativos, que el proceso tiene publicado en la intranet en el siguiente Link Controles Administrativos NTC-ISO 27001:2013 Anexo A, que consistió en verificar la(s) evidencia(s) relacionadas que soportan el cumplimiento de cada control. Frente a cada uno de ellos se emitió un resultado con los hallazgos preliminares, que fueron enviados al responsable de tecnología vía correo el jueves 14 de julio, el cual tuvo respuesta el viernes 15 de julio de 2022, con las observaciones y aclaraciones respectivas.

Se evidenció fortaleza en los controles relacionados con la definición de las políticas para la seguridad de la información, la definición y actualización del listado de los contactos de autoridades para reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley, la identificación de la propiedad de activos y las reglas establecidas para su uso y la revisión independiente a intervalos planificados del sistema de seguridad que se tiene implementado.

A.5. Políticas de la Seguridad de la Información	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información	A.5.1.2	Revisión a la Política de Seguridad de la Información

Hallazgo 2:
No se cuenta con evidencia de la revisión a la Política de Seguridad de la Información establecida en septiembre 19 de 2017, y que se tenía prevista efectuar para septiembre de 2019, según la declaración de aplicabilidad publicada en la intranet, de fecha de actualización 2019-02-18, para asegurar que continúa siendo adecuada, idónea y eficaz.

A.6. Organización de la Seguridad de la Información	A.6.1. Organización Interna	A.6.1.1	Roles y responsabilidades para la Seguridad de la Información

Observación 1.
Se evidencian las responsabilidades para la seguridad de la información, toda vez que se remite al documento denominado, MANUAL RESPONSABILIDADES DEL SGSI http://intranet.cnsc.net/phocadownload/Nuevo_SIG/FEB/m-sg-si-001_responsabilidades-del-sgsi_v1_20180413_pdf.pdf.y a la Resolución Interna 20171200058225 en donde definen responsabilidades, deberes y/o compromisos del SGSI que deben cumplir, la alta dirección, funcionarios y/o contratistas. Sin embargo se debe revisar que se tenga definido para los demás participantes, relacionado con quien hace que en materia de Seguridad de la información incluso acogiendo lo definido en el MSPI, que indica se debe definir un responsable de la seguridad y privacidad de la información y el equipo humano necesario para coordinar la implementación del MSPI; y en caso que el cargo no existe en la Entidad deberá ser delegado por acto administrativo y deberá depender de un área estratégica que no sea la Oficina o Dirección de Tecnología (se recomienda el despacho de nominador).

A.6. Organización de la Seguridad de la Información	A.6.1. Organización Interna	A.6.1.5	Seguridad de la Información en la Gestión de Proyectos

Hallazgo 3:
No se evidencia los requisitos establecidos para mantener la seguridad de la información en la gestión de los proyectos, según lo revisado en el proyecto OnBase, de acuerdo con lo solicitado por el modelo NTC-ISO 27001:2013 Anexo A numeral A.6.1.5 Seguridad de la Información en la Gestión de Proyectos.

A.6. Organización de la Seguridad de la Información	A.6.2. Dispositivos Móviles y Teletrabajo	A.6.2.2	Teletrabajo

Observación 2
Se evidencian las medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo, se hace por VPN. La modalidad de teletrabajo hasta ahora no se está trabajando en la CNSC, sin embargo, es conveniente comenzar a desarrollar las medidas de seguridad adecuadas para implementar la modalidad de Teletrabajo.

A.7. Seguridad de los	A.7.1. Antes de Asumir el Empleo	A.7.1.2	Términos y condiciones del empleo

Recursos Humanos			

Observación 3
Se cuentan con documentos para llevar a cabo la vinculación de servidores públicos Vinculación y Desvinculación de personal P-TH-001 y proceso de contratación de contratista, por lo que es recomendable revisar tales documentos para asegurar que se incluyen; la ley 21952 de 2019 y la ley 2094 de 2021, con el fin de evidenciar la comprobación de los antecedentes de todos los candidatos antes de asumir el empleo de acuerdo con dichas las leyes, normativa y códigos éticos que sean de aplicación, teniendo en cuenta la clasificación de la información a la que tendrá acceso y los riesgos percibidos, así como las obligaciones contractuales para los servidores y contratistas los términos y requisitos relacionados a la seguridad de la información, que deben cumplir. Para tal efecto, se requiere que las dependencias que generan la información reporten oportunamente a la DTIC, para mantener actualizada la información y acceso a los sistemas, pues sin este insumo se corre el riesgo de tener usuarios que no deben tener acceso a la información de la CNSC.

A.7. Seguridad de los Recursos Humanos	A.7.2. Durante la Ejecución del Empleo	A.7.2.1	Responsabilidades de la Dirección

Observación 4.
Se evidencia la necesidad que desde la alta dirección se asegure el cumplimiento por parte de los contratistas y servidores públicos de las políticas y procedimientos establecidos en la Comisión Nacional del Servicio Civil.

Se evidenció que desde Talento Humano se generó un radicado memorando No. 20196000008863 Orfeo frente al memorando de TICS de radicado número 20191300003813 Asunto Solicitud de información para el SGSI, se traslada esta responsabilidad a la "Alta Dirección".

A.7. Seguridad de los Recursos Humanos	A.7.2. Durante la Ejecución del Empleo	A.7.2.2	Toma de Conciencia, Educación y Formación en la Seguridad de la Información

Observación 5 Se deben realizar capacitaciones y/o concientizaciones que permitan afianzar los conocimientos relacionados con los requisitos de seguridad que empleados y contratistas deben implementar desde sus puestos de trabajo, lo cual permitirá asegurar que los boletines son leídos y entendidos, y lo más importante se están implementando, para de esa manera asegurar que se tiene controlados las amenazas que pueden llegar por ese medio.

Se evidencian las actividades que se han efectuado de concienciación en la CNSC, en lo referente a seguridad de la información, como son los boletines de la intranet de temas como Aumento de las amenazas por correo electrónico del 28 de junio de 2022, Alerta de Malware para Android del 15 de junio de 2022.

A.7. Seguridad de los	A.7.2. Durante la Ejecución del Empleo	A.7.2.3	Proceso Disciplinario

Recursos Humanos			

Observación 6
Se cuenta con un proceso / procedimiento DISCIPLINARIO ORDINARIO Y VERBAL Código: P-TH-006 Versión: 4.0 en el marco del proceso de gestión de talento humano que requiere ser actualizado, teniendo en cuenta que se relaciona la Ley 734 de 2002 (anterior Código Disciplinario Único), esta norma fue derogada con la Ley 1952 de 2019, en el citado procedimiento no se incluyó la Ley 1952 de 2019. Adicionalmente, es importante contar con un procedimiento que recoja las acciones a tomar ante aquellos funcionarios y/o contratistas que hayan provocado alguna brecha de seguridad, de acuerdo con lo solicitado por el modelo NTC-ISO 27001:2013 Anexo A numeral A.7.2.3 Proceso Disciplinario

A.7. Seguridad de los Recursos Humanos	A.7.3. Terminación y Cambio de Empleo	A.7.3.1	Terminación o cambio de responsabilidades de empleo

Observación 7
Se evidencia la generación del Memorando 20191300003813, de Solicitud de Oficina Asesora de Informática a Talento Humano para la implementación por parte de esa oficina de requisitos del SGSI el memorando fue respondido con el memorando 20196000008863. Sin atenderse la totalidad del requisito “Terminación o Cambio de Responsabilidades de Empleo: La CNSC tiene establecido el formato F-IT-004 (Paz y salvo y devolución de elementos y otras novedades), que al momento de presentar al jefe inmediato se debe realizar solicito de retiro, cancelación o modificación de usuarios según sea el caso, por tanto, se sugiere que se revise la funcionalidad del formato en compañía de la Oficina Asesora de Planeación”.

Se debe asegurar que efectivamente existe una comunicación clara en la terminación y/o cambio de empleo de las responsabilidades que incluyan los requerimientos de seguridad, las responsabilidades legales incluyendo los contenidos en los Acuerdos de Confidencialidad y en los Términos y Condiciones del empleo los cuales deben continuar por un período establecido después de la terminación de los contratos, según se evidenció con la líder del proyecto OnBase que continuaba configurada en el software de prueba.

A.8. Gestión de Activos	A.8.1. Responsabilidad por los Activos	A.8.1.1	Inventario de activos

Observación 8
Es importante revisar la pertinencia de incluir y mantener actualizado el inventario de activos en el cómo son: el software Onbase, la UPS 00066, el rack 2838 de almacenamiento y el banco de ítems, de acuerdo con el inventario que se tiene actualizado con fecha 2020-11-30, publicado en la intranet en el enlace http://intranet.cnsc.net/index.php/sistema-integrado-de-gestion/gestion-de-activos-de-la-informacion-sig . que relaciona un total 2319 activos.

No se está dando cumplimiento a la revisión anual planteada en el procedimiento GESTIÓN DE ACTIVOS DE LA INFORMACIÓN P-TI-SSI-003 Versión: 2.0. Aunque en el mismo procedimiento en la actividad 15, se establece que se hace bimestral.

A.8. Gestión de Activos	A.8.1. Responsabilidad por los Activos	A.8.1.3	Uso aceptable de los activos

Observación 9.
Se evidencia el INSTRUCTIVO PARA EL USO ADECUADO DE LOS RECURSOS TECNOLÓGICOS I-TI-002 Versión: 1.0 de fecha 31/10/2018, que describe los lineamientos que se deben tener en cuenta para recibir, operar, mantener y retornar los recursos de tecnología. Se debe asegurar las reglas de uso aceptable deben ser provistas por la Dirección, Empleados y funcionarios de terceras partes que utilizan o tienen acceso a los activos de la compañía deben ser conscientes de los límites para el uso de la información de la compañía, los activos asociados con instalaciones de procesamiento de esta, y otros recursos. conscientes de los límites para el uso de la información de la compañía, los activos asociados con instalaciones de procesamiento de esta, y otros recursos.

A.8. Gestión de Activos	A.8.1. Responsabilidad por los Activos	A.8.1.4	Devolución de Activos

Observación 10.
Se evidencia el INSTRUCTIVO PARA EL USO ADECUADO DE LOS RECURSOS TECNOLÓGICOS I-TI-002 Versión: 1.0 de fecha 31/10/2018, que describe los lineamientos que se deben tener en cuenta para recibir, operar, mantener y retornar los recursos de tecnología, Se debe verificar y asegurar que en equipo con la Dirección de Apoyo Corporativo - DAC se tenga cumpla con lo definido en la actividad 25 del procedimiento de activos y la generación del Aprobar formato finalización (ver actividad 26) y Certificado de entrega de elementos y otras novedades Ver actividad 27)

A.8. Gestión de Activos	A.8.2. Clasificación de la Información	A.8.2.2	Etiquetado y manejo de información

Hallazgo 4:
No se evidencia el procedimiento (s) para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización, según lo solicitado por la NTC-ISO 27001:2013 Anexo A, A.8.2.2 Etiquetado y manejo de información.

A.15. Relaciones con los Proveedores	A.15.1. Seguridad de la Información en las Relaciones con los Proveedores	A.15.1.3	Cadena de Suministro de Tecnología de Información y Comunicación

Observación 11
Se hace necesaria la implementación de los requisitos establecidos con proveedores o terceros que permita hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos, que permitan evidenciar su cumplimiento, como en el caso del contrato No. 080 de 2021 cuyo objeto es adquirir servicios de conectividad de acceso a internet mediante un canal de contingencia del canal principal de internet.

A.15. Relaciones con los Proveedores	A.15.2. Gestión de la Prestación de los Servicios de Proveedores	A.15.2.1	Control y revisión de la provisión de servicios del proveedor

Observación 12
Se hace necesario evidenciar y validar la implementación del CONTROL, REVISIÓN Y AUDITORÍAS efectuada a terceros para la provisión de servicios, según se evidencia en el servicio que se presta en el marco del contrato (contrato No. 080 de 2021 cuyo objeto es adquirir servicios de conectividad de acceso a internet mediante un canal de contingencia del canal principal de internet), el contrato 489 de 2020, con la empresa GIGA COLOMBIA S.A.S y contrato de prestación de servicios No. 086 de 2022, cuyo objeto fue: prestar servicios en modalidad de bolsa de horas para mantenimiento y desarrollos adicionales del gestor documental OnBase, según lo solicitado por modelo NTC-ISO 27001:2013 Anexo A, A.15.2.1 Control y revisión de la provisión de servicios del proveedor

A.15. Relaciones con los Proveedores	A.15.2. Gestión de la Prestación de los Servicios de Proveedores	A.15.2.2	Gestión de Cambios en los Servicios de los Proveedores

Observación 13
La gestión de cambios se constituye en un factor crítico de seguridad como parte de la provisión del servicio por lo que debe ser tenida en cuenta para la celebración de contratos que afecten la seguridad de la información y las comunicaciones, en donde se incluyan el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.

A.17. Continuidad de Seguridad de la Información	A.17.1. Continuidad de Seguridad de la Información	A.17.1.1	Planificación de la continuidad de la Seguridad de la Información

Observación 14
Se menciona que se cuenta con análisis del impacto al negocio (en diseño) Relación de elementos críticos de TI (en diseño) Identificación de cifras críticas de control (RTO y RPO) para la entidad (en diseño). Y se cuenta con el documento Operación del Plan de Recuperación ante Desastres - DRP (Disaster Recovery Plan) de TI G-TI-006.

Se debe complementar mediante el análisis de los riesgos y los procesos críticos, a fin de determinar e implementar las necesidades de seguridad de la información en términos de los diferentes planes de continuidad, que permitan contrarrestar los efectos de falla que puedan causar interrupciones de las actividades la CNSC.

A.17. Continuidad de Seguridad de la Información	A.17.1. Continuidad de Seguridad de la Información	A.17.1.2	Implementación de la continuidad de la seguridad de la información

Observación 15
Se debe implementar el análisis de los riesgos y los procesos críticos, con el fin de determinar e implementar las necesidades de seguridad de la información en términos de los diferentes planes de continuidad, que permitan contrarrestar los efectos de falla que puedan causar interrupciones de las actividades la CNSC.

A.18. Cumplimiento	A.18.1. Cumplimiento de Requisitos Legales y Contractuales	A.18.1.2	Derechos de propiedad intelectual (DPI)

Observación 16
Se debe verificar la política que ha establecido la CNSC y los procedimientos que garanticen el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

A.18. Cumplimiento	A.18.1. Cumplimiento de Requisitos Legales y Contractuales	A.18.1.4	Privacidad y Protección de información de datos personales

Observación 17
Se evidencia la publicación de la política de seguridad de la información en el siguiente link https://www.cnsc.gov.co/sites/default/files/202201/politica_de_tratamiento_de_proteccion_de_datos_personales-1_0.pdf. Sin embargo, se debe validar su implementación más teniendo en cuenta que esta labor es transversal a la CNSC.

Controles técnicos

Con respecto a los controles técnicos de la ISO 27001, se llevaron a cabo mesas de trabajo para verificar la aplicación efectiva de algunos de los controles, según se describe en los siguientes apartados.

Es preciso aclarar que adjunto a este informe se encuentra una matriz detallada con la totalidad de controles, tanto administrativos como técnicos, con la evidencia de la aplicación de cada uno de ellos a nivel documental.

A.9. Control de Acceso	A.9.1 Requisitos de negocio para el control de acceso	A.9.1.1	Política de control de acceso

En la Intranet, en la sección "Seguridad de la Información" se encuentra publicado el documento "Políticas de Direccionamiento Estratégico del SGSI" con código M-TI-SSI-002, Versión: 3.0 Fecha: 03/03/2022. Este documento contiene el capítulo “5.1.2 Política para Acceso Remoto para Ejecución de Actividades” donde se indica:

“*A la fecha de publicación de esta versión del documento, la modalidad de Teletrabajo NO está regulada en la Entidad y por tanto su ejecución no está contemplada como una forma de trabajo valida o legalmente reconocida*.”

Observación 18
Teniendo en cuenta que desde el mes de febrero se han otorgado posibilidades a funcionarios y contratistas de trabajar en una modalidad diferente a la presencial, se recomienda revisar el párrafo mencionado anteriormente dentro de la política y verificar elementos que puedan ser necesarios incluirse.

A.9. Control de Acceso	A.9.2. Gestión de acceso de usuarios	A.9.2.1	Registro y cancelación del registro de usuarios

Con el fin de verificar lo relacionado con el control de acceso a usuarios que han terminado su vinculación con la entidad, se procedió a revisar aleatoriamente en la herramienta GLPI la efectiva desvinculación de algunas personas que durante el mes de junio de 2022 finalizaron su contrato de prestación de servicios, encontrando que lo siguiente:

Identificación	Nombre	Tiquetes de GLPI relacionados	Observación
1018470409	DANIEL ALEJANDRO NEIRA SIERRA	*Ticket# 98852 07-07-2022*	A través del ticket se solicitó la activación del usuario luego de la terminación del contrato, pero no se indica el motivo de la solicitud ni la fecha hasta la cual se debe extender el acceso.
1072714441	MARIA CAMILA GODOY RODRIGUEZ	*Ticket# 98559 01-07-2022*	A través del ticket se solicitó la activación del usuario luego de la terminación del contrato, pero no se indica el motivo de la solicitud ni la fecha hasta la cual se debe extender el acceso.
Varios	Usuarios múltiples	*Ticket# 98486 30-06-2022*	En este ticket se solicita prórroga para mantener activos a 16 usuarios hasta el 8 de julio. No se observa la justificación para esta solicitud.
Varios	Usuarios múltiples	*Ticket# 98837 07-07-2022*	En este ticket se solicita prórroga para mantener activos a 8 usuarios hasta el 15 de julio. No se observa la justificación para esta solicitud.

Observación 19
Se recomienda incluir en el ticket la información suficiente para que el analista de soporte pueda dar cumplimiento a lo expresado en el instructivo relacionado, en cuanto a verificar que las condiciones y características de la modificación radicada sean viables tanto en los aspectos técnicos, como en los términos de seguridad informática que se encuentren vigentes en la dependencia y la entidad.

De otra parte, se efectuó en GLPI una revisión de las solicitudes asociadas al sistema OnBase, con los siguientes resultados:

Categoría del ticket	Total tickets
5. Software > On-Base	244
5. Software > On-Base > Acceso	62
5. Software > On-Base > Asesoría procedimental	28
5. Software > On-Base > Capacitación	7
5. Software > On-Base > Creación / modificación / eliminación de usuarios	265
5. Software > On-Base > Instalación	28
Total general	**634**

El periodo de consulta fue desde noviembre de 2021, fecha del inicio de operación de OnBase, hasta julio de 2022. Se observa que se registraron 634 tickets, de los cuales 265 correspondieron a gestión de acceso a usuarios, sin embargo, revisando el detalle, en las otras categorías también se encontraron solicitudes mixtas en las cuales también se gestionaban usuarios, pero dado que se solicitaban varios servicios en el mismo ticket no fue posible cuantificarlos.

De las anteriores cifras se concluye que hay un alto volumen de solicitudes que se relacionan con la solicitud de acceso o retiro del aplicativo, por lo cual se recomienda que, como parte del proceso de vinculación / desvinculación, se incluya un punto de chequeo para activar / desactivar al usuario, de tal manera que el jefe del usuario no deba realizar una solicitud adicional, disminuyendo así el número de solicitudes.

A.9. Control de Acceso	A.9.2. Gestión de acceso de usuarios	A.9.2.3	Gestión de derechos de acceso privilegiado

Observación 20
Dentro de la documentación del proceso y en las Políticas de direccionamiento estratégico del SGSI, no se observó un procedimiento de autorización particular para los usuarios que deben tener acceso privilegiado, por ejemplo, aquellos que serán administradores en los aplicativos misionales o de apoyo como OnBase.

A.9. Control de Acceso	A.9.3 Responsabilidades de los usuarios	A.9.3.1	Uso de información de autenticación secreta

Observación 21
No se están aplicando políticas para exigir que se utilicen caracteres especiales dentro de las contraseñas, siendo esta una buena práctica para generar contraseñas seguras.

De otra parte, se sugiere implementar una política para que no se utilice la misma contraseña en los sistemas de apoyo y en los sistemas misionales.

A.9. Control de Acceso	A.9.4. Control de Acceso a Sistemas y Aplicaciones	A.9.4.3	Sistema de gestión de contraseñas

Observación 22
Se encontró la publicación en la Intranet de una nota (http://intranet.cnsc.net/index.php/noticias/1885-la-importancia-de-tener-contrasenas-fuertes) con fecha 21 Abril de 2022, en la cual la DTIC recomienda cambiar periódicamente la contraseña (al menos una vez cada 30 días), sin embargo, esto no debe ser una recomendación sino una práctica que se aplique de forma regular, dado que las buenas prácticas indican que las contraseñas se deben cambiar e impedir su reuso.

A.11 Seguridad física y del entorno	A.11.1. Áreas Seguras	A.11.1.2	Controles de acceso físicos

En visita realizada al Centro de cómputo (o Data center) por parte de los auditores William Lara y Yaneth Montoya, el día 14 de julio de 2022, y atendida por el ingeniero Jose Vicente Sarmiento y el ingeniero Javier Alberto Rojas se pudo observar lo siguiente:

- El acceso al Data center se realiza a través de personas que tengan carnet o huella.
- Se cuenta con una bitácora para registrar el acceso de los visitantes, la cual contiene un primer registro de fecha 28 de septiembre de 2018 y el último registro era del 13 de julio de 2022 relacionado con un mantenimiento del CCTV.
- Se cuenta con 3 UPS, una para equipos y dos para servidores.
- Se tiene como contingencia la planta eléctrica del edificio.
- Se evidencia que los centros de cableado están debidamente marcados.

- Se tienen 4 fuentes de energía trifásica, las cuales incluyen tomas, iluminación, equipos de Data center y aires acondicionados.
- Se informa a los auditores que se tienen 21 sensores de humo que activan la alarma si dos de ellos que no estén juntos, detectan el peligro.
- Se encontró un extintor apto para equipos eléctricos, cuya fecha de vencimiento es en noviembre de 2022. Se informa a los auditores que la puerta de acceso al Data center es contra incendio.
- El espacio cuenta con un sistema para control de incendios.
- El Data center incluye racks para las Ups, centros de cableado, discos para backups, servidores HP, aires acondicionados. servidores en hiperconvergencia y servicio de Internet.
- El área del Data center se encuentra aislada con dos equipos de aire acondicionado que se activan de forma alterna en caso de que uno de ellos falle.
- No se observan puertas adicionales a la de entrada o ventanas en las instalaciones.
- Se encontraron cajas y un armario con cintas de backup.
- Se informa a los auditores que al Data center accede el proveedor de Internet, dado que los equipos se encuentran allí, así como la empresa de seguridad de la entidad.
- Se observa una cámara afuera de la entrada al Data center, la cual es monitoreada por el servicio de vigilancia de la entidad.
- Se observa que la puerta de acceso al Data center queda justo en frente de las puertas de los baños a los cuales pueden acceder personas externas a la entidad.

Observación 23
Con relación a los controles asociados a la seguridad física, se recomienda establecer la viabilidad para que las instalaciones de procesamiento de información gestionadas por la organización estén separadas físicamente de las gestionadas por partes externas.

A.11 Seguridad física y del entorno	A.11.1. Áreas Seguras	A.11.1.3	Seguridad de oficinas, recintos e instalaciones

Nota: dentro del alcance de esta auditoría no se definió la visita o revisión de seguridad en oficinas, por lo cual se recomienda realizar una revisión por parte de la DTIC con respecto a los sitios de trabajo donde se realizan actividades o se maneja información confidencial, para evitar que sean visibles y audibles desde el exterior.

A.11 Seguridad física y del entorno	A.11.2. Equipos	A.11.2.5	Retiro de activos

Observación 24
No se encontraron evidencias de la socialización del Protocolo para el uso de dispositivos tecnológicos fuera de las instalaciones de la CNSC, código: PR-TI-004, versión: 1.0, fecha: 21/09/2020, para las personas que utilizan equipo portátil u otros dispositivos contemplados en el alcance del mencionado documento.

A.11 Seguridad física y del entorno	A.11.2. Equipos	A.11.2.8	Equipos de usuario desatendidos

Observación 25
Aunque en el "Instructivo para el uso adecuado de los recursos tecnológicos", Código I-RT- 002, Versión: 1.0, Fecha: 31/10/2018, se establece que se debe bloquear la sesión de trabajo del computador cuando el funcionario necesite levantarse de su puesto de trabajo por un periodo

considerable o pierda la visibilidad del mismo, la frase “por un periodo considerable” puede ser ambigua, por lo cual se recomienda que se aclare que siempre que el funcionario se levante de su puesto deje bloqueada su sesión.

A.12. Seguridad de las Operaciones	A.12.1. Procedimientos Operacionales y Responsabilidades	A.12.1.1	Procedimientos de operación documentados

Observación 26
No se encontró un registro histórico de la documentación del proceso, donde se evidencie, por ejemplo, que un documento que antes estaba a nivel de procedimiento, ahora es un instructivo o una guía. Por ejemplo, el "Instructivo para gestionar la capacidad de TI", código: I-TI-013, versión: 1.0, fecha: 30/04/2022, no es la primera versión del documento, dado que antes las actividades relacionadas se encontraban vigentes a nivel de procedimiento (P-TI-009, versión: 1.0, fecha: 06/11/2019).

A.12. Seguridad de las Operaciones	A.12.1. Procedimientos Operacionales y Responsabilidades	A.12.1.2	Gestión de cambios

Observación 27
Aun cuando se cuenta con el procedimiento Gestión de Cambios de TI, código: P-TI-002, versión: 3.0, fecha: 23/03/2022, el cual aplica para recursos tecnológicos, no se tienen en cuenta los cambios en la organización y en los procesos de negocio, como componente importante de los cambios.

A.12. Seguridad de las Operaciones	A.12.2. Protección Contra Código Malicioso	A.12.2.1	Controles contra códigos maliciosos

El día 7 de julio de 2022 se realizó una mesa de trabajo con el equipo de la DTIC encargado de la consola de antivirus, reunión que fue atendida principalmente por el ingeniero Luis Fernando Otalora y en la cual se pudo observar lo siguiente:

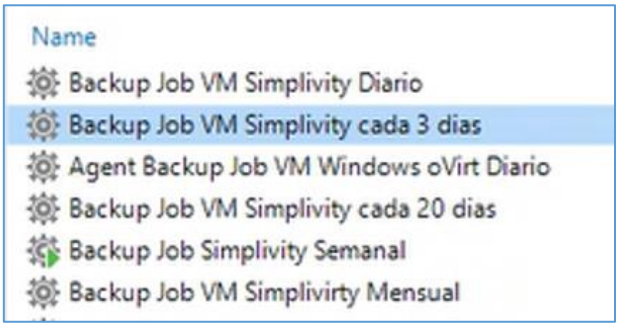
- El antivirus que está en uso actualmente es Cylance de Blackberry.
- La consola permite ver en una línea de tiempo las amenazas que el antivirus ha detectado.
- No se observaron amenazas activas.
- El sistema se basa en una lista genérica con posibles amenazas, mediante la cual se puede verificar si otros fabricantes de antivirus lo consideran una amenaza. Se observa que la lista fue actualizada por última vez el 04 de julio de 2022.
- En la consola se manejan “Zonas” y en ella se tienen configurados los equipos de la entidad a partir de las diferentes ubicaciones como Montevideo o piso 7 (calle 96).
- En la consola pueden configurarse políticas de seguridad a través de grupos llamados “Fases” que permiten aumentar o disminuir el nivel de protección. Se observa la siguiente cantidad de equipos por cada tipo:
    - Default = 4 equipos
    - Fase 1 = 2 equipos
    - Fase 2 = 61 equipos
    - Fase 3 = 371 equipos
    - Fase 4 = 0 equipos
- No se encuentran incluidos equipos en Fase 4 que es donde se configurarían restricciones con relación a dispositivos externos como USB o discos duros externos.

- La solución no está desplegada en servidores de desarrollo y pruebas.
- Para la Fase 3 no se encuentra activo el Control de aplicaciones. Según indica el ingeniero Luis Fernando se consultó con el fabricante de Cylance e indicó que esa funcionalidad podría generar problemas, por ejemplo, archivos de Excel con macros, y sugirió desactivarla.

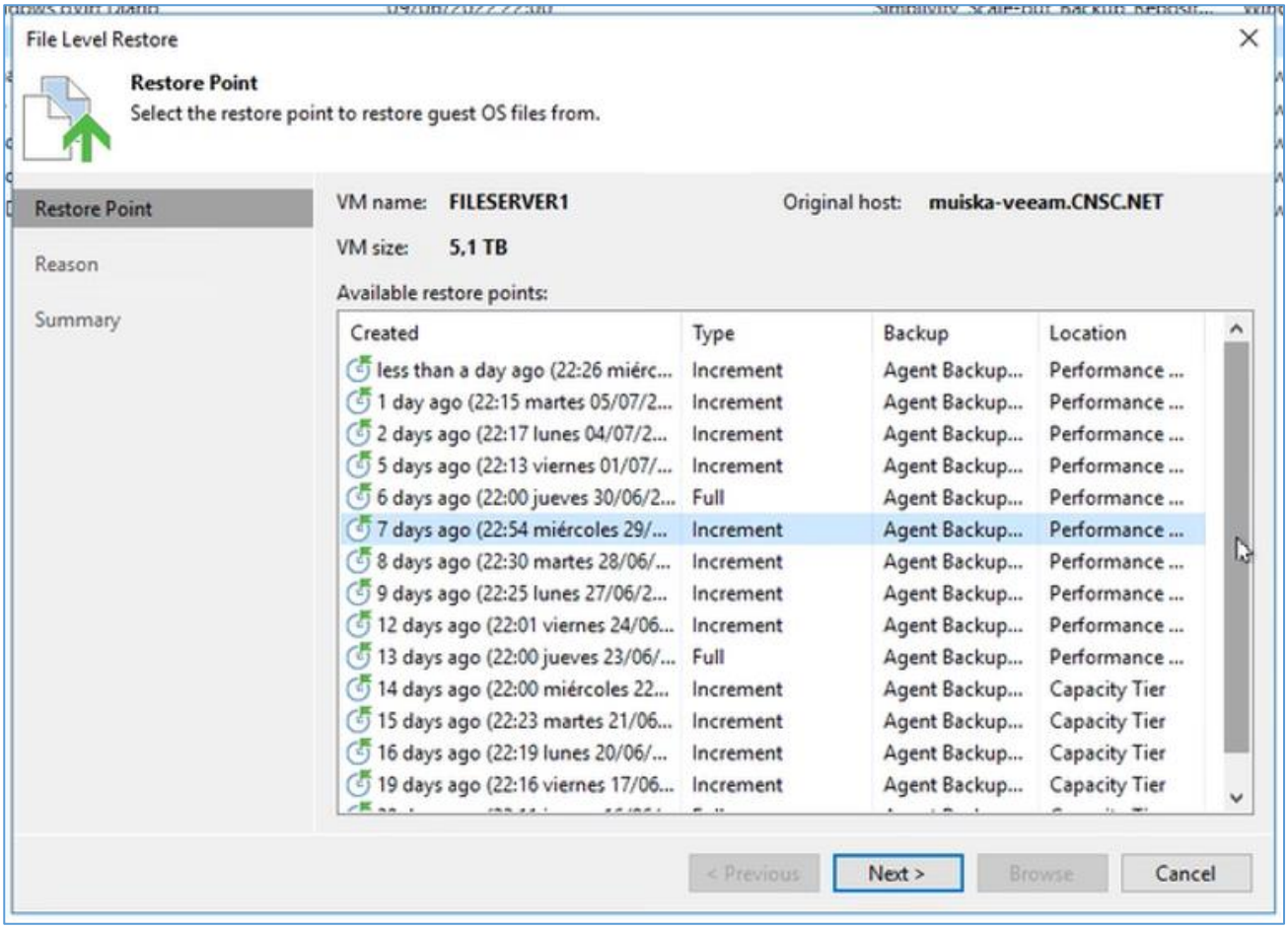
Observación 28
Teniendo en cuenta que las memorias USB o los discos externos representan una amenaza por la posibilidad de infección a los computadores de la entidad con software malicioso, se recomienda activar el control para el análisis de cualquier dispositivo externo antes de su uso.

A.12. Seguridad de las Operaciones	A.12.3. Copias de Respaldo	A.12.3.1	Respaldo de la información

Se llevó a cabo una mesa de trabajo el 7 de julio de 2022 para conocer los aspectos técnicos relacionados con el backup. Se encontró que dependiendo de la plataforma se tiene una periodicidad diferente para ejecutar el backup (por restricciones de confidencialidad se presenta sólo una sección de la imagen tomada a la plataforma durante la reunión):



Se pudo evidenciar la ejecución correcta de diferentes backups:



Se realizó una prueba a este control eliminando un archivo del file server y solicitando su restauración a través de la mesa de servicios, con el número **GLPI 98950**. La prueba de recuperación fue exitosa, verificando que el backup realizado con anterioridad contenía efectivamente el archivo eliminado.

El alcance de este control en la norma ISO 27001 incluye el almacenamiento posterior de los backups en medios externos, el cual en la entidad se realiza a través de cintas. Estas cintas se deben almacenar en un lugar remoto, a una distancia suficiente que permita evitar el impacto de un daño que pueda ocurrir en el sitio principal donde se generan los backups.

Durante la visita al Data center se observó que las cintas de backup de años anteriores se encuentran dentro de esas mismas instalaciones. Posterior a la visita se informó a la auditoría que se encontraban en revisión los estudios previos para una contratación por mínima cuantía con el objeto de prestar servicios para la custodia de estos medios.

Hallazgo 5:
Se encontraron cintas de backup en el Data center de la entidad, incumpliendo lo establecido en la Guía Estrategia institucional de copias de seguridad de la información de la CNSC, código: G-TI-005, con relación a la custodia de estas, así como con la implementación del control A.12.3.1 Respaldo de la información de la ISO 27001.

A.12. Seguridad de las Operaciones	A.12.6. Gestión de la Vulnerabilidad Técnica	A.12.6.1	Gestión de las vulnerabilidades técnicas

Durante el año 2021 se ejecutó un contrato cuyo objeto era “Prestar los servicios especializados de Ethical hacking, análisis de vulnerabilidades y pruebas de ingeniería social para la Comisión Nacional del Servicio Civil – CNSC”. Según indicaron los funcionarios de la DTIC durante la auditoría, no se tiene prevista una nueva contratación para realizar este tipo de pruebas, pero se están realizando pruebas con herramientas libres.

Observación 29
Se recomienda ejecutar de forma regular actividades para llevar a cabo análisis de vulnerabilidades, teniendo en cuenta que diariamente surgen nuevas amenazas.

A.13. Seguridad de las Comunicaciones	A.13.1 Gestión de la Seguridad de las Redes	A.13.1.2	Seguridad en los servicios de red

Observación 30
No se encontraron documentados los requisitos de red segmentados por tipos de usuario. Según se indica en este control: se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

A.13. Seguridad de las Comunicaciones	A.13.2 Transferencia de Información	A.13.2.2	Acuerdos sobre transferencia de Información

Observación 31
Se tiene el formato "Acuerdo de confidencialidad y no divulgación", código: F-DE-SGQ-011, versión: 2.0, fecha: 30/03/2022, sin embargo, este no contiene elementos suficientes para:

- Definir los procedimientos para asegurar trazabilidad y no repudio.
- Definir los estándares técnicos mínimos para empaquetado y transmisión.
- Tener certificados de depósito de títulos en garantía.
- Establecer los estándares de identificación de mensajería.
- Definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos.
- Establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente.
- Definir las normas técnicas para registro y lectura de información y software.
- Cualquier control especial que se requiera para proteger elementos críticos, tales como criptografía.
- Mantener una cadena de custodia para la información mientras está en tránsito.
- Definir los niveles aceptables de control de acceso.

A.13. Seguridad de las Comunicaciones	A.13.2 Transferencia de Información	A.13.2.3	Mensajería electrónica

Observación 32
Aunque se cuenta con el protocolo "Uso interno de la mensajería instantánea", código: PR-TI-002, versión: 2.0, fecha: 16/03/2020, no se encontraron evidencias de su socialización, en especial con personal nuevo en la entidad.

Adicionalmente, no se han definido los requisitos para firmas electrónicas, teniendo en cuenta que esto hace parte integral de la mensajería electrónica.

A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas.	A.14.1. Requisitos de Seguridad de los Sistemas de Información.	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información

En el documento "Políticas de direccionamiento estratégico del SGSI", capítulo 5.1.8 Política de Desarrollo Seguro, se establecen lineamientos para el desarrollo interno de aplicaciones. También existe el “Protocolo para el levantamiento de información para desarrollos de software”, código: PR-TI-006, versión: 1.0, fecha: 09/03/2022 donde se indica que es necesario que durante la etapa de levantamiento de información sean identificadas las condiciones de seguridad. En el procedimiento "Desarrollo de sistemas de información", código: P-TI-005, versión: 6.0, fecha: 26/11/2021, se indica que el registro de requerimientos se realiza a través del formato "Análisis de requerimientos funcionales".

El formato “Análisis de requerimientos funcionales”, código: F-TI-004, versión: 2.0, fecha: 12/01/2021 hace mención a “Elementos de Seguridad” en la sección Metodología por Casos de Uso, sin embargo, esto no aparece en la sección Metodología por Historia de Usuario.

Observación 33
Los requisitos relacionados con seguridad de la información siempre se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes, independiente de la metodología de desarrollo que se utilice. Aunque la indicación anterior aparece en varios documentos, se recomienda reforzar el tema en los formatos de levantamiento de requerimientos.

A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas.	A.14.2. Seguridad en los Procesos de Desarrollo y de Soporte.	A.14.2.6	Ambiente de desarrollo seguro

Observación 34
Se tiene la "Guía para la gestión de los ambientes de trabajo para desarrollo", código: G-TI-007, versión: 1.0, fecha: 22/11/2021, sin embargo, no se encontraron evaluaciones frente a los riesgos de los ambientes, para lograr una implementación efectiva del control.

A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas.	A.14.3. Datos de Prueba.	A.14.3.1	Protección de datos de prueba

Observación 35
Los lineamientos generales sobre datos de prueba se relacionan en la "Guía para la gestión de los ambientes de trabajo para desarrollo", código: G-TI-007, versión: 1.0, fecha: 22/11/2021; sin embargo, no se hace mención a lo siguiente:

- Autorización separada cada vez que se copia información operacional a un ambiente de pruebas.
- Precisar que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.
- Establecer que el copiado y uso de la información operacional requiere un rastro de auditoría.

Criterios auditados

1. https://www.cnsc.gov.co/sites/default/files/documentos/peti-actualizacion2022.pdf

   Plan estratégico de tecnologías de información (actualización 2022)

2. https://www.cnsc.gov.co/sites/default/files/documentos/plan_seguridad_y_privacidad_de_la_informacion_cnsc_2022.pdf

   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.

3. https://www.cnsc.gov.co/sites/default/files/documentos/programacion_plan_anual_de_accion_2022_v3.pdf

   El plan de acción de la CNSC establecido para la vigencia 2022 versión 3

4. http://intranet.cnsc.net/phocadownload/2022/MAR/2021%20%204%20trimestre%20seguimientos%20proyectos%20inversion.pdf

   Seguimiento a los proyectos de inversión

5. https://www.cnsc.gov.co/transparencia/planeacion/plan-estrategico

   Plan estratégico institucional 2020 - 2022

6. https://www.cnsc.gov.co/sites/default/files/documentos/plan-institucional-de-archivos-pinar1.pdf

   Plan Institucional de Archivos - PINAR 2019 – 2022 versión 1.2 marzo de 2020

7. Acuerdo No 003 de 2015 estableció los lineamientos generales en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos y profirió la guía para la formulación de metadatos, las cuales conforman la base para la creación, diseño y mantenimiento del esquema de metadatos para la gestión de documentos al interior de las entidades públicas

8. Circular 04 de 2010 de la Comisión intersectorial de Políticas y de Gestión de la Información para la Administración Pública-COINFO,

9. El Decreto No. 2609 de 2012, regula la gestión documental para todas las entidades del Estado, en temas como: la gestión de documentos en sus diferentes soportes físicos y electrónicos, principios, políticas y procesos de la gestión documental, instrumentos archivísticos y las características de los sistemas de gestión documental, entre otros aspectos.

10. Artículo 5 de la Ley 2052 de 2020, las entidades públicas, así como los particulares que cumplan funciones públicas y/o administrativas, deben automatizar y digitalizar la gestión interna de los trámites que adelanten cumpliendo con los plazos establecidos en el Decreto 088 de 2022, la CNSC requiere automatizar algunos de sus trámites y/o servicios, haciendo uso a la plataforma OnBase.

11. Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones Titulo 9. Política de Gobierno Digital. habilitadores
12. Norma Técnica Colombiana NTC/ISO 15489-1
13. Acuerdo 039 de 2002 Por el cual se regula el procedimiento para la elaboración y aplicación de las Tablas de Retención Documental
14. Ley 594 de 2000 Ley General de Archivos y se dictan otras disposiciones.

3. CONCLUSIONES DE LA AUDITORÍA

- El proceso de Gestión Tecnológica de la información y las comunicaciones presenta debilidades en su documentación que se reflejan en la publicación de documentos identificados con misma revisión, pero cuyo contendido es diferente, procedimientos que no establecen los registros que deben quedar producto de la actividad, y formatos de registros que no están concatenados a documentos base.

- La estructuración y aprobación del proyecto OnBase planteó los objetivos buscados con su implementación, por lo que se debe, como parte del modelo de maduración del proyecto medir los resultados alcanzados y documentar las lecciones aprendidas, en el marco de la gestión del conocimiento del SIG.

- El programa SGDEA OnBase permitió mejorar requerimientos frente al sistema ORFEO como son; parametrización de actividades sin necesidad de conocimiento especializado de programación, balanceo de cargas o distribución de tareas, autenticidad de las comunicaciones mediante firma digital, tecnologías para migración de información ante cambios de tecnologías, estandarización y automatización de trámites, interoperabilidad con otros sistemas, la generación de reportes y por último para destacar el cumplimiento por parte de los documentos de atributos de ley que lo hacen convertirse en documentos con valor probatorio.

- La definición del proyecto para la migración de la documentación que se encuentra en Orfeo, de tal manera que la Comisión, cuente con un solo repositorio, para efectos de evitar la duplicidad de acciones para el mantenimiento y administración que implica tener dos softwares para el manejo de la documentación, disminuir el riesgo de y agilizar la transferencia del conocimiento.

- La muestra efectuada para la mesa de servicios, arrojó un porcentaje de cumplimiento del 80%, 4 tickets tienen la fecha de respuesta superior a la fecha de solución, superando de esa manera el tiempo parametrizado y asignado para el acuerdo de nivel de servicio /ANS, un análisis más afondo de las razones que impactaron el cumplimiento del ANS, su tipología, los inconvenientes al usuario, y a la seguridad de la información, permitirá concluir acerca de la gestión de la mesa de servicio y catálogo, tarea que debe ser abordada en la siguiente auditoría.

- El uso de la herramienta GLPI, debe ser fortalecido en lo referente lección aprendida en la base de conocimientos, que permita continuar el aprendizaje y por ende optimizar los ANS.

- El objetivo relacionado con evaluación de la conformidad del sistema de gestión de seguridad de la información, en lo relacionado a los controles del anexo A, se ajustó para auditar lo relacionado únicamente con el cumplimiento de los documentos y procedimientos exigidos por el modelo, dado el grado de madurez del sistema, el cual está en una etapa temprana para evaluar su mantenimiento y

mejora. Es necesario la participación activa de otras áreas como Talento Humano, DAC, Oficina Asesora Jurídica para incrementar y evidenciar la implementación de los controles que en materia de seguridad de la información y las comunicaciones se tienen previstas desde la oficina de TICS, y que siendo una actividad transversal de su compromiso y aplicación depende el logro de la política de SGSI y los objetivos planteados.

4. HALLAZGOS

Hallazgo 1
Con relación al proyecto OnBase, no se encontró documentación que permitiera evidenciar la trazabilidad en los cambios efectuados a dicho sistema, lo cual genera un riesgo frente al control sobre los ajustes, configuraciones, parametrizaciones, personalizaciones y/o desarrollos que se están realizando sobre el software. Lo anterior representa un incumplimiento al procedimiento GESTIÓN DE CAMBIOS DE TI, P-TI-002 Versión: 3.0.

Hallazgo 2
No se cuenta con evidencia de la revisión a la Política de Seguridad de la Información establecida en septiembre 19 de 2017, y que se tenía prevista efectuar para septiembre de 2019, según la declaración de aplicabilidad publicada en la intranet, de fecha de actualización 2019-02-18, para asegurar que continúa siendo adecuada, idónea y eficaz; según lo solicitado por modelo NTC-ISO 27001:2013, Anexo A, A.5.1.2 Revisión a la Política de Seguridad de la Información.

Hallazgo 3
No se evidencia los requisitos establecidos para mantener la seguridad de la información en la gestión de los proyectos, según lo revisado en el proyecto OnBase, de acuerdo con lo solicitado por el modelo NTC-ISO 27001:2013 Anexo A numeral A.6.1.5 Seguridad de la Información en la Gestión de Proyectos.

Hallazgo 4
No se evidencia el procedimiento (s) para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización, según lo solicitado por modelo NTC-ISO 27001:2013 Anexo A, A.8.2.2 Etiquetado y manejo de información.

Hallazgo 5
Se encontraron cintas de backup en el Data center de la entidad, incumpliendo lo establecido en la Guía Estrategia institucional de copias de seguridad de la información de la CNSC, código: G-TI-005, con relación a la custodia de estas, así como con la implementación del control A.12.3.1 Respaldo de la información de la NTC-ISO 27001:2013.

5. RECOMENDACIONES

- La documentación del proceso debe continuar ajustándose a los criterios que tiene establecido el Sistema Integrado de Gestión, específicamente en el Procedimiento Elaboración y Control de Documentos y Registros - P-DE-SGQ-005 y Guía para la Elaboración y Control de Documentos y Registros - G-SG-001 , en lo referente al control de versiones para garantizar la publicación únicamente de versiones actualizadas, identificar los registros que deben generarse producto de las actividades establecidas en la documentación,

- Se aprueban y distribuyen documentos que tienen el mismo número de revisión, con información diferente. Se debe enlazar desde el documento origen donde se establece la directriz, el formato(s) que se tienen para tal propósito con el fin de que el usuario conozca a donde remitirse y se cuente con esa secuencia documental. Tal y como se presenta con el documento denominado GUÍA POLÍTICAS OPERACIONALES DE TI G-TI-004 Versión: 1.0 de Fecha: 27/07/2020, y el que establece la necesidad de firmar un acuerdo de confidencialidad con terceros, formato Acuerdo de Confidencialidad y No divulgación - F-DE-SGQ-011.

- Los controles relacionados con los siguientes numerales mantienen fortalezas evidenciadas en la documentación establecida, y cuya implementación y puesta en práctica debe mejorarse, con el fin de que se pueda evidenciar un sistema de gestión, que mantiene y mejora. A.5.1.1 **Documento de Política de Seguridad de la Información,** A.6.1.2 Separación de Deberes, **A.6.1.3** Contacto con las autoridades, **A.6.1.4** Contacto con grupos de interés especial, **A.6.2.1** Política para dispositivos móviles, **A.7.1.1** Etiquetado y manejo de información, A.8.2.2 Etiquetado y manejo de información, A.8.2.3 Manipulado de la información, A.8.3.1 Gestión de Medios, A.8.3.2 Removibles, Disposición. Para los demás controles administrativos se debe revisar la planificación y las estrategias usadas, para encontrar los ajustes necesarios que permitan mejorar su implementación.

6. PLAN DE MEJORAMIENTO

Como mecanismo de control la Dirección de Tecnologías de la Información y las Comunicaciones deberá elaborar un plan de mejoramiento, tendiente a generar acciones correctivas frente a cada hallazgo y las acciones requeridas frente a las observaciones. Este plan deberá ser presentado a la Oficina de Control Interno máximo tres (3) días hábiles después de la fecha de entrega del informe final de la auditoría.

7. ANEXOS

Listado de controles administrativos y técnicos de la NTC-ISO 27001:2013

Elaboró	Aprobó
ORIGINAL FIRMADO	ORIGINAL FIRMADO
YANETH MONTOYA GARCÍA Auditora	
ORIGINAL FIRMADO	
WILLIAM LARA PALACIOS Auditor	**YOLANDA CASTRO SALCEDO** Jefe de Oficina de Control Interno