Fecha del Informe Final	**Día**	**31**	**Mes**	**12**	**Año**	**2024**
Nombre de la actividad	Auditoría interna de gestión a los procesos: ▪ *"Gobierno y Gestión de Datos e Información"* actividades claves de éxito *"Gestionar TI"* y *"Gestionar Seguridad y Privacidad de los Datos e Información"*. ▪ *"Gestión de Bienes y Servicios"* en relación con los contratos suscritos para presta los servicios de nube publica y nube privada de la SNS de las vigencias 2023 y 2024.					
Objetivo de la Auditoría	La presente auditoría tiene como objetivo dar a conocer a la Alta Dirección el estado de gestión de la seguridad de la información y privacidad la información, así como la operación de los Sistemas de Información de la Superintendencia Nacional de Salud, para lo cual se procederá a evaluar las soluciones tecnológicas, seguridad de la información y la gestión de los sistemas o aplicativos que son utilizados por áreas misionales y de apoyo mediante el desarrollo de las siguientes actividades: • Evaluación de los Sistemas de información seleccionados por muestreo, validando: ▪ Niveles de acceso de usuarios. ▪ Entrada-proceso-salida de información. ▪ Reportes y consultas. ▪ Seguridad de la información. ▪ Copias de seguridad de cada sistema. • Seguimiento al Plan de Continuidad del Negocio (Análisis de Impacto Empresarial - BIA), plan de contingencia de la entidad, plan de seguridad y privacidad de la información y actualizaciones de procesos y actividades claves de éxito liderados por STI. • Seguimiento a la Matriz de Riesgos de Seguridad y Privacidad de la Información dentro del alcance de la presente auditoria • Manejo de incidentes de Seguridad de la información presentados dentro del alcance de esta auditoría y medidas establecidas para atender este tipo de eventos con su respectiva documentación (Manuales, guías, instructivos, etc.). • Seguimiento a la gestión realizada por la Subdirección de Tecnologías de la Información frente a los hallazgos y recomendaciones identificados en la auditoria a sistemas de información realizada en la vigencia 2023. • Verificación de la ejecución de los contratos suscritos para prestar los servicios de nube pública y nube privada de la SNS de las vigencias 2023 y lo corrido de 2024.					
Alcance	El alcance en tiempo de la presente auditoría corresponde al período comprendido entre el 1 de enero a 31 de diciembre de 2023 y del 1 de enero 31 de julio de 2024.					
Criterios	Los criterios de auditoría para tener en cuenta por parte de la Oficina de Control Interno son: ▪ Decreto 1080 de 2021. ▪ Decreto 1078 de 2015 ▪ Resolución 00500 de 2021 ▪ Resolución 1519 de 2020 ▪ Decreto 648 de 2017. ▪ Resolución 14909 de 2020. ▪ Decreto 1499 de 2017. ▪ Ley 80 de1993 y demás que las modifiquen o complementen.					

Carrera 68 A Nº 24 B - 10, Torre 3 - Pisos 4, 9 y 10 | PBX +57 601 744 2000 • Bogotá D.C.
www.supersalud.gov.co

	▪ Validación de la seguridad, confidencialidad, integridad y disponibilidad de los sistemas de información seleccionados. ▪ Norma Técnica Colombiana ISO-IEC 27001:2022. Conforme en el desarrollo de auditoría, podrán ser tenidos en cuenta criterios adicionales que tengan relación con los sistemas de información objeto de esta auditoría.
Auditor	Juan Carlos Nocua Camargo – Profesional Especializado (auditor líder)
Tabla de Contenido	

1. INFORME

Con el fin de cumplir los fines y cometidos trazados en el ejercicio de auditoría interna que ahora nos ocupa, en especial las funciones asignadas por la Ley 87 de 1993 y demás normas aplicables, así como las actividades definidas para la vigencia 2024 en el Plan Anual de Auditorías y Seguimientos (PAAS) de la Oficina de Control Interno, el auditor de la Oficina de Control Interno procedió a efectuar los análisis del caso, respecto de los procesos *"Gobierno y Gestión de Datos e Información" actividades claves de éxito" Gestionar TI" y "Gestionar Seguridad y Privacidad de los Datos e Información"* y "*Gestión de Bienes y Servicios*" en relación con los contratos suscritos para prestar los servicios de nube publica y nube privada de la SNS de las vigencias 2023 y 2024; lo anterior a partir de lo preceptuado en la Resolución No. 20231200200011126-6 de 2023 *"Por la cual se modifica el mapa de procesos de la Superintendencia Nacional de Salud".*

El alcance de la presente auditoría es el correspondiente a la vigencia 2023 y del 1 de enero al 30 de julio de 2024. En este sentido por parte del auditor se evidenció una buena disposición y participación por parte de la Dirección de Innovación y Desarrollo y la Subdirección de Tecnologías de la información en el desarrollo y ejecución de la auditoria de Gobierno y Gestión de Datos e Información.

1.1 Gestión realizada por la Subdirección de Tecnologías de la Información frente a los hallazgos y recomendaciones identificados en la auditoría a sistemas 2023

En desarrollo del presente ítem se hizo validación y seguimiento a las acciones adelantadas por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnologías de la Información, frente a las observaciones y no conformidades determinadas en la auditoría a los sistemas de información de la Superintendencia Nacional de Salud, realizada por la Oficina de Control Interno durante la vigencia 2023, con el siguiente resultado:

Así las cosas, se solicitó a la STI aportar información y evidencias del acogimiento o no de los hallazgos determinados con radicado No. 20241400000080393_solicitud2_INF_2024, los cuales se registran a continuación con el correspondiente análisis de la Oficina de Control Interno:

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
OBSERVACION	1	*"2.2.1 Debilidad en la formalización de entrega de cargos de exfuncionarios de la Dirección de Innovación y Desarrollo y la Subdirección de Tecnologías de la Información."*	*"En la relación de informes de entrega de cargo tanto de directivos (de la DID y STI) como de funcionarios que trabajaron en la STI, el equipo auditor de la Oficina de Control Interno evidenció que los informes de gestión y de entrega de cargo enunciados, no se encontró formalización de entrega ni en el módulo de actas de ITS ni en SuperArgo."*	*"Los informes fueron entregados en su momento al superior inmediato, tener presente que las coordinaciones solo iniciaron desde el 11 de diciembre de 2023"*	El auditor evidenció que no hay transferencia de conocimiento y no está consolidada una base de conocimiento y los integrantes del grupo de seguridad de la información se conformaron en diciembre de 2023 y del total funcionarios asignados al grupo de seguridad solo se encontró a tres funcionarios que no dan abasto con el cumplimiento de las políticas de seguridad digital y gobierno digital, por último no se aprobado la matriz de roles y responsabilidades de la Seguridad y privacidad de la Información y de TI. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera **Observación N°.1. Debilidad en la formalización de entrega de cargos de exfuncionarios de la Dirección de Innovación y Desarrollo y la Subdirección de Tecnologías de la Información.** de ***"Gobierno y Gestión de Datos e Información"*** de la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno insta a la SNS -DID/STI a que tome acciones correctivas e inmediatas para fortalecer el grupo de seguridad de la información y se realice los roles y responsabilidades de Seguridad y privacidad de la Información de la SNS. Con el fin de garantizar la Seguridad y Privacidad de la Información.

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
OBSERVACION	2	*"2.2.2 Debilidad en la aplicación de controles relacionados con políticas de seguridad."*	*De la trazabilidad de las acciones realizadas para atender el incidente de seguridad del 17/02/2023, y específicamente tomando las recomendaciones formuladas por COLCERT en informe de marzo de 2023, el equipo auditor de la OCI evidenció debilidad en la aplicación de controles relacionados con políticas de seguridad, entre otras, para:* *▪ De organización de la seguridad de la información.* *▪ De gestión de activos.* *▪ De control de acceso.* *▪ Contra códigos maliciosos.* *▪ Para los recursos tecnológicos.* *▪ Para seguridad de los servicios de red.* *▪ De seguridad de las comunicaciones.* *▪ Para adquisición desarrollo y mantenimiento de sistemas.* *Por lo descrito, es importante y urgente que la STI tome acciones correctivas e inmediatas para verificar, definir y aplicar políticas de seguridad que resguarden los sistemas de información, servidores e infraestructura de la entidad, en aras de mitigar al máximo la materialización de riesgos, como consecuencia de ataques de seguridad como los ocurridos en 2023."*		El Auditor de la Oficina de Control Interno de acuerdo con los soportes y evidencias aportados por la DID/STI, evidenció lo siguiente: un informe del COLCERT de marzo de 2023 con el análisis y acciones correctivas del incidente de seguridad del 17 de febrero de 2023, 2 informes del incidente por parte de subdirectores del momento de la STI los cuales no coincidieron en algunos concepto y no se evidenció documento con toda la traza de las acciones adelantadas por parte de la entidad para subsanar, remediar y contener el incidente de seguridad de la información, además la DID/STI no soportaron el cumplimiento de los controles relacionados con las Políticas de seguridad digital de la SNS, aunado al hecho de que el auditor no evidenció documentos actualizados, guías procedimientos, transferencia de conocimiento ni base de conocimientos y lecciones aprendidas del incidente de seguridad del 17 de febrero de 2023. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera **Observación No 2. Debilidad en el cumplimiento en la aplicación de controles relacionados con políticas de seguridad y privacidad de la información** de *"Gobierno y Gestión de Datos e Información"* de la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno insta a la DID/STI tome acciones correctivas e inmediatas para verificar, definir y aplicar políticas de seguridad que resguarden los sistemas de información, servidores e infraestructura de la entidad, en aras de mitigar al máximo la materialización de riesgos, como consecuencia de ataques de seguridad como los ocurridos en 2023.

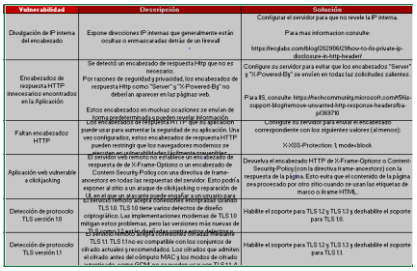
Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
OBSERVACION	3	*"2.2.3 Debilidad en la implementación de una metodología estructurada para la atención de incidentes de seguridad de la información", que contenga por lo menos un "plan de contingencia", un "plan de recuperación de desastres o incidentes", y un "plan de continuidad del negocio"*	*"De la revisión de las actividades desarrolladas por la DID y la STI para la atención de los incidentes de 2023, si bien se adelantaron actividades conducentes a la atención de los eventos, recuperación de los sistemas e infraestructura y, a tomar medidas para minimizar el impacto que generen nuevos ataques, es importante que se defina un modelo de gestión de incidentes de seguridad de la información, que incluya aspectos como la "ciberseguridad", por lo que el equipo auditor de la OCI considera necesario y urgente que se establezca una metodología para la "atención de incidentes de seguridad de la información", así como del "plan de contingencia" un "plan de recuperación de desastres o incidentes", y un "plan de continuidad del negocio", que permitan definir estructuradamente las acciones que se deben adelantar cuando se presenten este tipo de incidentes, lo que también permitirá crear una base de conocimiento para futuros eventos, independientemente de las personas que lideren o tengan a cargo estos temas.* *Adicionalmente, esta observación se sustenta en las recomendaciones formuladas por COLCERT, CSIRT, COINSA y de los mismos informes de gestión de entrega de los subdirectores de T.I. y de DID que estuvieron en el primer semestre de 2023, y dada la*	*"El procedimiento para la atención de incidentes hace parte del plan de trabajo que se encuentra en ejecución"*	El auditor verifico la información aportada por la DID/STI de las actividades desarrolladas por la DID y la STI para la atención de los incidentes de 2023, si bien se adelantaron actividades conducentes a la atención de los eventos, recuperación de los sistemas e infraestructura y, a tomar medidas para minimizar el impacto que generen nuevos ataques, El auditor evidencio incumplimiento de lo que define el Manual Para la Prestación del Servicio Para la Atención De Incidentes - DIMN13 en los siguientes aspectos: En la entrada del incidente; el registro, clasificación, Diagnostico, resolución y cierre del incidente En cuanto el seguimiento y la Monitorización del Incidente El auditor no evidenció matriz de roles y responsabilidades de atención de incidentes tanto para la vigencia 2023 como del 1 de enero hasta el 30 de noviembre de 2024, además no se evidencio que se documentara los incidentes del 17 de febrero de 2023 y 12 de septiembre de 2023 como también no se aportó soportes o evidencia de información de este incidente por parte DID/STI . el auditor no evidencio validación y análisis del incidente que fue catalogado como incidente mayor, en relación con la cantidad de usuarios afectados, la criticidad de los servicios afectados y su tiempo de afectación o caída de servicio afectando el principio de disponibilidad de la información . No se evidencio que se haya escalado el incidente de seguridad identificado como incidente mayor como lo establece la clave de éxito "gestionar TI" y que direcciona a la clave de éxito "Gestionar Problemas y Cambio", el auditor evidencio que la DID/STI no aporto documentación de lo que establece la actividad clave de éxito "Gestionar Problemas y Cambios" . No se identificó la información relacionada con el incidente (actas de cambio, aceptación del área usuaria, etc.) para su respectivo registro en la base de datos de errores conocidos y su documentación en la base de datos de conocimiento. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera **No Conformidad No. 1. Incumplimiento de Articulo 9 Gestion de incidentes de la resolución 00500 de 2021** del proceso **"***Gobierno y Gestión de Datos e Información***"** de la actividad *clave de éxito "Gestiona*r, Problemas y Cambios" liderado por la Dirección de Innovación y

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			importancia que ellas implican para la entidad en la mitigación de riesgos de seguridad, en el numeral 1.4 "Aplicación de una metodología estructurada para el manejo de incidentes de seguridad" de este informe, se detalla y complementa esta Observación, adicionalmente exponiendo la necesidad de tomar decisiones administrativas y gestiones ante la alta dirección, que permitan implementar medidas técnicas, operativas, legales, organizacionales, determinando el paso a paso de cada acción y estableciendo roles y responsabilidades, por lo que se solicita consultar el numeral 1.4."		Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno eleva no conformidad al proceso "Gobierno y Gestion de Datos de Información" - actividad clave de éxito "Gestionar problemas y cambios" liderado por la Dirección de innovación Desarrollo y al proceso "Direccionamiento estratégico" liderado por Oficina Asesora de Planeación, ante el incumplimiento preceptuado en el Articulo 9 Gestión de incidentes de la resolución 00500 de 2021 al no gestionarse incidentes de seguridad y privacidad de la información con oportunidad, y calidad frente a la transferencia de conocimiento, Base de conocimiento (lecciones aprendidas), una adecuada gestión de riesgos, seguimiento y monitoreo a la gestión de incidentes y actualización de procedimientos definidos para atender dichos incidentes aspecto que resulta importante intervenir que permitirán manejar adecuadamente situaciones como las presentadas en 2023, logrando mitigar de manera acertada la materialización de riesgos, y con los cuales se podría generar una base de conocimientos para garantizar la integridad, confidencialidad, y la disponibilidad de los sistemas de información y de infraestructuras.
OBSERVACION	4	*"2.2.4 Debilidad en el seguimiento a las acciones determinadas en los Puestos de Mando Unificados (PMU) realizados con ocasión de los incidentes de seguridad, de 2023."*	*"En cuanto a las observaciones y recomendaciones formuladas por entes externos líderes en ciberseguridad, el equipo auditor de la Oficina de Control Interno estima conveniente e importante que el PMU tome atenta nota de las recomendaciones formuladas por los funcionarios de CSIRT y COLCERT, para que la entidad establezca acciones urgentes, las que finalmente redundarán en una mejora continua, logrando garantizar la seguridad, confidencialidad, integridad y disponibilidad de los servicios de la entidad."*		El auditor de la Oficina de Control Interno evidenció soportes o evidencias de las acciones que realizaron en el Puesto de Mando Unificado de la SNS, con respecto de las recomendaciones formuladas por los funcionarios de CSIRT y COLCERT *"análisis de Vulnerabilidades SNS Marzo 2023"*, como lo es consolidar el grupo de seguridad de la información, fortalecer las herramientas de ciberseguridad y consolidar los roles y responsabilidades del grupo de la STI, dar cumplimiento a los lineamientos dados por MINTIC y DAFP, en cuento al manejo de la tecnología. *"Recomendaciones generales para resolver y prevenir vulnerabilidades como las encontradas durante las pruebas realizadas.* *▪ Dentro de lo posible mantener actualizadas las aplicaciones utilizadas en el servidor con los últimos parches de seguridad liberados por el fabricante.* *▪ Ofuscar el código de la página para que no pueda ser visto y/o modificado. .* *▪ Se recomienda implementar ajustar los flags del encabezado HTTP con el fin de mitigar posibles ataques.*

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
					▪ *Cambiar los tipos de cifrado utilizados en el sitio ya que los usados actualmente cuentan con vulnerabilidades que ponen en riesgo la integridad, disponibilidad y confidencialidad de la información.* ▪ *Realizar un plan de remediación de las vulnerabilidades encontradas.* ▪ *Realizar pruebas de seguridad periódicas, no sólo para asegurar que las vulnerabilidades detectadas en auditorías anteriores han sido subsanadas, sino también para detectar nuevas vulnerabilidades que hayan podido aparecer debido a los cambios en las aplicaciones y/o infraestructura, así como la multitud de vulnerabilidades que se descubren a diario en sistemas operativos y software en general "* Se evidenció que la mayoría de las recomendaciones dadas por COLCERT no fueron acatadas y no se generaron acciones para poder subsanar las situaciones allí reflejadas. Con fundamento en lo anteriormente expuesto, la Oficina de Control Interno genera **Observación N°. 3. Debilidad en el cumplimiento por parte de PMU de las recomendaciones de CSIRT y COLCERT**. de ***"Gobierno y Gestión de Datos e Información"*** de la actividad *"Gestionar Problemas y Cambios"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La OCI insta a que por parte de Puesto de Mando Unificado se tomen decisiones administrativas, operativas y gestiones ante la alta dirección para dar cumplimiento a las recomendaciones establecidas por los entes externos de apoyo para el manejo de incidente de seguridad y privacidad de la información como lo son CSIRT y COLCERT, igualmente se documenten y hagan parte de la base de conocimiento de la gestión de incidentes de seguridad de la SNS, con el fin de garantizar la Confidencialidad, Integridad y la disponibilidad de la Información de la SNS.
OBSERVACION	5	*"2.2.5 Falta de definición y aprobación de documentos sobre "Roles y responsabilidades", "manual de Seguridad de la información".*	*La Oficina de Control Interno hizo verificación de los documentos aportados por el ing. Jaime Duarte con el documento de entrega de cargo (Roles y responsabilidades, manual de Seguridad de la información), observando que son borradores o proyectos*	*"Estos documentos fueron gestionados por el funcionario Jaime Duarte, sin embargo, no fueron entregadas las últimas versiones para*	El auditor de la Oficina de Control Interno hizo verificación de los documentos aportados por DID/STI (Roles y responsabilidades de la Seguridad y Privacidad de la Información), observando que son proyectos de los mismos, por consiguiente, los roles y responsabilidades que se encuentran en el documento aportado por STI describen las funciones establecidas en el decreto 1080 de 2021 y no están diligenciados por el formato - DEFT12 *"MATRIZ DE ROLES Y*

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			de los mismos y no están aprobados por la Oficina Asesora de Planeación ni incluidos en el Sistema Integrado de Gestión – SIG, por lo que se sugiere a la Subdirección de Tecnologías de la Información analizar la viabilidad de su implementación, y de considerarlo pertinente, realizar las gestiones pertinentes con la Oficina Asesora de Planeación para su aprobación e integración al SIG.	*solicitar la inclusión en el SIG"*	*RESPONSABILIDADES"* definido por la OAP, igualmente, no han sido aprobados por la Oficina Asesora de Planeación ni incluidos en el Sistema Integrado de Gestión – SIG, para que posteriormente sean aprobados por el señor Superintendente Nacional de Salud y el Comité de Gestión y Desempeño Institucional. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **No Conformidad N°. 2. Incumplimiento de la definición de roles y responsabilidades de Seguridad y Privacidad de la información y de TI de la SNS.** al proceso **"***Gobierno y Gestión de Datos e Información***"** de la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: Realizado el análisis de la información objetiva aportada por el proceso objeto de evaluación independiente, no se observó el diligenciamiento del Formato "*DEFT12 – Matriz de Roles y Responsabilidades*" por parte del proceso "*Gobierno y Gestión de Datos e Información*" a cargo de la Dirección de Innovación y desarrollo, como también lo es que, no se logró identificar el seguimiento y revisión a cargo del proceso "*Direccionamiento Estratégico*" liderado por la Oficina Asesora de Planeación, aunado a la debilidad en el principio de *"Autocontrol"* que dispone el "*Modelo Estándar de Control Interno (MECI)",* esto por parte del proceso para detectar desviaciones y con ello efectuar correctivos para la adecuada ejecución de las actividades y/o tareas bajo su responsabilidad, y que representan oportunidad de mejora para el adecuado desarrollo de las Actividad Clave de Éxito objeto de análisis y evaluación
OBSERVACION	6	*"2.2.6 Debilidad en el monitoreo y análisis de vulnerabilidades a los sistemas de información, servidores e infraestructura de la entidad."*	*"El auditor de la Oficina de Control Interno considera necesario que la Subdirección de Tecnologías de la Información como acción correctiva, establezca un procedimiento para realizar periódicamente, y cuando sea necesario extemporáneamente, sobre el análisis acerca de las vulnerabilidades técnicas de los sistemas de información y de la infraestructura de la entidad, con el fin de*	*"El procedimiento de pruebas de seguridad y remediación hace parte del plan de trabajo que se encuentra en ejecución."*	El Auditor de la Oficina de Control Interno verificó los documentos aportados por DID/STI de los Análisis de Vulnerabilidades de las aplicaciones y de la Infraestructura de la SNS, encontrando lo siguiente: Análisis de Vulnerabilidades realizado en el mes de marzo de 2023 realizado por COLSERT. Las pruebas las realizaron sobre las siguientes URL. • https://superargo.supersalud.gov.co •https://pqrdsuperargo.supersalud.gov.co • https://nrvcc.supersalud.gov.co • https://www.supersalud.gov.co •https://gestionhumana.supersalud.gov.co

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			determinar oportunamente y evaluar la exposición que tiene la Entidad ante potenciales vulnerabilidades, y así tomar las medidas apropiadas para tratar el (los) riesgo (s) asociado (s).”		El informe suscrito al respecto dio recomendaciones con el fin de que la Supersalud - Superintendencia Nacional de Salud las tenga presentes y pueda llegar a mitigar el riesgo existente sobre su infraestructura tecnológica. El análisis de vulnerabilidades realizado tuvo los siguientes objetivos específicos: ▪ Comprobación del estado de la seguridad en los servicios, mediante el descubrimiento de vulnerabilidades existentes que puedan comprometer la seguridad en términos de Confidencialidad de la información, la Integridad de los datos y de la Disponibilidad de los servicios ofrecidos. ▪ Posibles puntos de mejora para corregir o contrarrestar el impacto que podrían tener la explotación de las vulnerabilidades. La metodología utilizada es la denominada CVE (Common Vulnerabilities and Exposures), estándar de clasificación y calificación de vulnerabilidades de aceptación mundial. Los resultados del análisis de seguridad de los sitios web evaluados y las pruebas de seguridad realizadas al sitio, identificaron 9 vulnerabilidades críticas, 11 vulnerabilidades Altas, 62 vulnerabilidades Medias y 30 vulnerabilidades Bajas. Las recomendaciones realizadas por COLCERT fueron las siguientes: *“▪. Mantener actualizadas las aplicaciones utilizadas en el servidor con los últimos parches de seguridad liberados por el fabricante.* *▪ Ofuscar el código de la página para que no pueda ser visto y/o modificado.* *▪ Se recomienda implementar ajustar los flags del encabezado HTTP con el fin de mitigar posibles ataques.* *▪ Cambiar los tipos de cifrado utilizados en el sitio ya que los usados actualmente cuentan con vulnerabilidades que ponen en riesgo la integridad, disponibilidad y confidencialidad de la información.* *▪ Realizar un plan de remediación de las vulnerabilidades encontradas.* *▪ Realizar pruebas de seguridad periódicas, no sólo para asegurar que las vulnerabilidades detectadas en auditorías anteriores han sido subsanadas, sino también para detectar nuevas vulnerabilidades que hayan podido aparecer debido a los cambios en las aplicaciones y/o infraestructura, así como la multitud de vulnerabilidades que se*

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
					descubren a diario en sistemas operativos y software en general." También realizaron lo siguiente: ▪ Escaneo de puertos. ▪ Análisis de Cabeceras HTTP Aplicaciones Web. Se hicieron igualmente las siguientes recomendaciones: *"Realizar escaneo de puertos para localizar los puntos de red cliente que contienen servicios web disponibles al público."* Del análisis de cabeceras HTTP se recomendó ajustar las cabeceras aplicaciones Web que no se encontraron con calificación A" que *es el más Seguro" y F el menos Seguro"* Por otro lado, del 24 al 28 de febrero de 2024 la DID/STI realizó análisis de vulnerabilidades a las siguientes aplicaciones: www.supersalud.gov.co intranet.supersalud.gov.co genesis.supersalud.gov.co nrvcc.supersalud.gov.co sivical.supersalud.gov.co En el documento se analizó, lo que se muestra en el siguiente cuadro:  Donde se observó que hay vulnerabilidades que fueron encontradas en el informe de marzo de 2023 realizado por COLCERT y que no fueron remediadas o subsanadas por la DID/STI, además no se evidenció documento soporte sobre las acciones realizadas para remediar o subsanar las vulnerabilidades identificadas tanto en el análisis de vulnerabilidades de COLCERT en marzo de 2023 y en el análisis realizado en febrero de 2024 por la DID/STI. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **Observación N°. 4. Debilidad en el cumplimiento de la realización de Análisis de Vulnerabilidades, monitoreo,**

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
					remediación y seguimiento de éstas. al proceso *"Gobierno y Gestión de Datos e Información"* de la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno considera necesario que la DID/STI o el responsable de la Seguridad y Privacidad de la información de la SNS, realice las Acciones de detección, además de las preventivas y correctivas y establezca un procedimiento para realizar periódicamente, el análisis acerca de las vulnerabilidades técnicas de los sistemas de información y de la infraestructura tecnológica de la entidad, con el fin de determinar oportunamente y evaluar la exposición que tiene la Entidad ante potenciales vulnerabilidades, y así tomar las medidas apropiadas para tratar el (los) riesgo (s) asociado (s).
OBSERVACION	7	*"2.2.7 Debilidad en la verificación de la actualización de antivirus, firewall y sistemas operativos de los servidores de las aplicaciones."*	*"El equipo auditor de la Oficina de Control Interno considera necesario que la Subdirección de Tecnologías de la Información como acción correctiva, establezca un procedimiento por el cual se conserven registros de manera permanente las actualizaciones antivirus, firewall, sistemas operativos de los servidores de las aplicaciones e infraestructura, con el fin de tener un histórico de las actividades realizadas por esa dependencia, con el fin de evaluar oportunamente la exposición que tiene la Entidad ante potenciales vulnerabilidades, y así tomar las medidas apropiadas para tratar el (los) riesgo (s) asociado (s)."*	*"Se realizó el mantenimiento de firewall - fortigate IFX generó parchado de los servidores virtuales IFX reanudó esquema de backups"*	El auditor de la Oficina de Control Interno realizó la verificación de acuerdo con los documentos y soportes suministrados por la DID/STI, no se observó registros de actualizaciones de antivirus, del firewall, sistemas operativos de los servidores de las aplicaciones e infraestructura, ni tampoco reportes de log de auditoría. y un procedimiento para realizar actividades de seguimiento y monitoreo. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera **Recomendación N°. 1. Debilidad en el registro de actualizaciones de antivirus, firewall y sistemas operativos de los servidores de las aplicaciones de la entidad.** de *"Gobierno y Gestión de Datos e Información"* de la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno considera necesario que la DID/STI o el responsable de la Seguridad y Privacidad de la información de la SNS, realice un procedimiento por el cual se conserven registros de manera permanente de las actualizaciones antivirus, firewall, sistemas operativos de los servidores de las aplicaciones e infraestructura, con el fin de tener un histórico de las actividades realizadas por DID/STI, a efectos de evaluar oportunamente la exposición que tiene la Entidad ante potenciales vulnerabilidades, y así tomar las medidas apropiadas para tratar el (los) riesgo (s) asociado (s).

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
OBSERVACION	8	*"2.2.8 Debilidad en la implementación de un documento que especifique los lineamientos para la realización de copias de seguridad, su tiempo de retención y del plan de recuperación de copias."*	*"En la revisión de la documentación aportada sobre la realización de copias de seguridad, su tiempo de retención y del plan de recuperación de copias, el equipo auditor de la Oficina de Control Interno considera pertinente y necesario que se establezca una metodología documentada, que defina estructuradamente las acciones a seguir para realizar estas actividades, lo que también permitirá crear una base de conocimiento para las personas que lideren o tengan a cargo estos temas.* *Así mismo, estos procedimientos permitirán detectar fallas oportunamente para tomar acciones de control y seguimiento con el fin de evitar la materialización de riesgos, que involucren la afectación de seguridad, integridad, y disponibilidad de la información, y además permitirá la oportuna y acertada toma de decisiones por las instancias pertinentes."*	*"El documento Manual para las copias de seguridad de la Información se entregó en la carpeta dispuesta por control interno para las evidencias"*	La Oficina de Control Interno en la revisión de la documentación aportada sobre la realización de copias de seguridad, su tiempo de retención y del plan de recuperación de copias, solo evidenció la actualización del Manual para las copias de seguridad de la Información – DIMN14 donde solo se aplicó al Proceso de restauración 2024 al aplicativo **Sivica**l del 14 de agosto de 2024 y no se aportaron las acciones y lineamientos definidos en el manual para todas las aplicaciones con su respectiva documentación y plan de recuperación . Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **Recomendación N°. 2. Debilidad en la aplicación del Manual para las copias de seguridad de la Información – DIMN14** al proceso de **"***Gobierno y Gestión de Datos e Información***"** en la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: la Oficina de Control Interno considera pertinente y necesario que la DID/STI cree una base de conocimiento con su respectiva transferencia. Así mismo, estos procedimientos permitirán detectar fallas oportunamente para tomar acciones de control y seguimiento con el fin de evitar la materialización de riesgos, que involucren la afectación de seguridad, integridad, y disponibilidad de la información.
OBSERVACION	9	"2.2.9 Debilidad para implementar acciones que permitan dar cumplimiento a lo establecido en la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, en relación con la protección de datos personales."	*"El equipo auditor de la Oficina de Control Interno considera pertinente que se tomen acciones tendientes a dar cumplimiento a los lineamientos de la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, dada la importancia de este tema para la seguridad, confidencialidad e integridad de la información de la SNS, sustentados en la trazabilidad de este informe en relación con los incidentes de seguridad presentados*		El auditor de la Oficina de Control Interno conforme a la información aportada por DID/STI no evidenció acciones relacionadas con la Protección de Datos Personales de la SNS, además, con Radicado **20231500000053943** del 19 de mayo de 2023 se realizaron recomendaciones para dar cumplimiento a lo que define la Ley 1581 de 2012, Ley de protección de Datos personales y el capítulo 26 del Decreto Único 1074 de 2015, el cual reglamentó la información mínima que debe contener el RNBD y los términos y condiciones bajo los cuales se deben inscribir en éste las bases de datos sujetas a la aplicación de la Ley 1581 de 2012". Estas disposiciones no fueron acogidas y se sigue presentando la misma situación evidenciada con el radicado de la referencia.

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			el 17/02/2023 y 12/09/2023."		Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **No Conformidad N°. 3 Incumplimiento de lo que establece la Ley 1581 de 2012 Ley de Protección de Datos** al proceso de *"Gobierno y Gestión de Datos e Información"* de la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así La Oficina de Control Interno eleva No conformidad por el incumplimiento de lo que establece la Ley 1581 de 2012, al proceso "gobierno y Gestion de Datos e Información" – actividad Clave de éxito Gestionar seguridad y privacidad de la información liderado por la Dirección de Innovación, no se evidencio políticas de protección de datos personales, no se encuentra definido procedimientos, manuales, Así mismo no se tiene definido y publicado el aviso de privacidad, se insta a la entidad que de manera prioritaria se tomen las acciones y medidas necesarias para dar cumplimiento a lo que establece la Ley 1581 de 2012 Ley de Protección de Datos Personales, con el fin de que la SNS no se vea abocada a la materialización de un riesgo que conlleve a sanciones de carácter Legal.
OBSERVACION	11	*"2.2.11 Debilidad en la supervisión del contrato 158 de 2022, suscrito con IFX Networks Colombia S.A.S."*	*"En la evaluación a la supervisión del contrato 158 de 2022 suscrito con IFX Networks Colombia S.A.S. se evidenció que al momento de la Auditoría y conforme con el seguimiento a la ejecución del contrato en comento, los supervisores del contrato enunciados en el numeral 1.7 de este informe, no habían subido a la plataforma de "Colombia compra eficiente" los informes de supervisión del contrato, correspondientes a los pagos de enero, febrero, marzo, abril, mayo, junio y julio; solamente estaba cargado el informe de supervisión del mes de diciembre de 2022, elaborado por el Supervisor Luis Carlos Ovalle Acosta. Igual situación se presenta*		El auditor de la Oficina de Control Interno no realizó ningún Análisis con respecto de esta Observación puesto que el contrato 158 de 2022 se terminó en el 2023.

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			frente a la documentación que soporta los pagos realizados que, a la fecha del presente informe de auditoría, no han sido subidos en dicho aplicativo, incumpliendo el deber de publicidad de las actuaciones inherentes a la ejecución del contrato. *En este punto es importante indicar que como hecho subsecuente de la presente auditoría, los informes que se acabaron de relacionar (los de la vigencia 2023), fueron publicados en la página de Colombia Compra Eficiente el 07/09/2023, evidenciándose inoportunidad en la gestión de supervisión de la Subdirección de Tecnologías de la Información."*		
OBSERVACION	12	*"2.2.12 Debilidad en el reporte de materialización de riesgos, por parte de la STI"*	*"En verificación de riesgos de gestión y corrupción de los procesos liderados por la STI tanto de la vigencia 2022 como los definidos para la vigencia 2023 (a cargo del proceso Gobierno y Gestión de Datos e Información liderado por la DID, pero que son ejecutados por la STI), se evidencia debilidad en el autocontrol que deben ejercer los líderes de procesos, ya que cuando un proceso detecta la materialización de sus riesgos, debe reportarlo a la OAP, registrarlo en ITS y por ende generar los planes de tratamiento con las acciones que sean necesarias para subsanar las causas-raíz que los originaron, en cumplimiento de la política de*		El auditor de la Oficina de Control Interno realizará el respectivo análisis en el capítulo de riesgos del presente informe.

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			administración de riesgos de la entidad."		
OBSERVACION	13	*"2.2.13 Falta de oportunidad en la generación de informes de monitoreo de los riesgos de seguridad y privacidad de la información."*	*"En verificación de riesgos de seguridad y privacidad de la información, el equipo auditor de la OCI evidenció debilidad en el monitoreo de los controles definidos en el tratamiento de riesgos de seguridad y privacidad de la información y en la no detección de materialización de riesgos, máxime que la STI es la líder operativa de este tema y son quienes identifican, analizan, formulan, evalúan y monitorean los riesgos de seguridad y privacidad de la información, a nivel institucional, incumpliendo lo establecido en la política de administración de riesgos de la entidad."*		El auditor de la Oficina de Control Interno realizará el respectivo análisis en el capítulo de riesgos del presente informe.
NO CONFORMIDAD	1	*"2.3.1 La Entidad no cuenta con una matriz de roles y responsabilidades y de segregación de funciones."*	*"En la verificación de la aplicación a los principios de seguridad de la información, es pertinente que la Subdirección de Tecnologías de la Información como acción correctiva, continúe con la definición de la matriz de roles y responsabilidades y de segregación de funciones para la seguridad de la información que permita asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información, hasta*	*Esta matriz hace parte de un plan de mejoramiento que está en cabeza de Jaime Duarte.*	El auditor de la Oficina de Control Interno hizo verificación de los documentos aportados por DID/STI (Roles y responsabilidades de la Seguridad y Privacidad de la Información), observando que son proyectos de los mismos, dado que, los roles y responsabilidades que se encuentran en el documento aportado por STI se describieron las funciones establecidas en el decreto 1080 de 2021 y no están diligenciados por el formato - DEFT12 *"Matriz de Roles Y Responsabilidades"* definido por la OAP. Igualmente, no han sido aprobados por la Oficina Asesora de Planeación ni incluidos en el Sistema Integrado de Gestión – SIG, para que posteriormente sean aprobados por el señor Superintendente Nacional de Salud y el Comité de Gestión y Desempeño Institucional.

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			su aprobación, publicación en el SIG e implementación en todas las instancias de la entidad, en aras de garantizar el actuar ante incidentes de seguridad, mitigando la materialización de riesgos por omisión y desconocimiento de las responsabilidades de todos los actores frente al tema."		Con fundamento en lo anteriormente expuesto, la Oficina de Control Interno **reitera la No Conformidad N°. 2. Incumplimiento de la definición de roles y responsabilidades de Seguridad y Privacidad de la información y de TI de la SNS.** al proceso de ***"Gobierno y Gestión de Datos e Información"*** en las actividades: *"Gestionar Seguridad y Privacidad de los Datos e Información"*, "*Gestionar Problemas y Cambios"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: Realizado el análisis de la información objetiva aportada por el proceso objeto de evaluación independiente, no se observó el diligenciamiento del Formato "*DEFT12 – Matriz de Roles y Responsabilidades*" por parte del proceso "*Gobierno y Gestión de Datos e Información*" a cargo de la Dirección de Innovación y desarrollo, como también lo es que, no se logró identificar el seguimiento y revisión a cargo del proceso "*Direccionamiento Estratégico*" liderado por la Oficina Asesora de Planeación, aunado a la debilidad en el principio de *"Autocontrol"* que dispone el "*Modelo Estándar de Control Interno (MECI)",* esto por parte del proceso para detectar desviaciones y con ello efectuar correctivos para la adecuada ejecución de las actividades y/o tareas bajo su responsabilidad, y que representan oportunidad de mejora para el adecuado desarrollo de las Actividad Clave de Éxito objeto de análisis y evaluación.

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
NO CONFORMIDAD	2	*"2.3.2 Materialización de riesgos de seguridad de la información, por vulneración de los principios de "Confidencialidad, Integridad y Disponibilidad", con los ataques cibernéticos de 2023; así mismo la materialización de riesgos de gestión definidos para la vigencia 2023."*	*"En la verificación de los compromisos definidos en la política del componente de seguridad de la información contenida en el Anexo del Manual de Políticas institucionales FIMN07 (ahora DEFT13), y de acuerdo con la trazabilidad de este informe relacionada con los incidentes de seguridad presentados el 17/02/2023 y 12/09/2023, estos compromisos se vieron afectados, ya que los principios de Confidencialidad, Integridad y Disponibilidad fueron vulnerados, por lo que se evidencia la materialización de riesgos de seguridad y privacidad de la información de la siguiente manera: NOTA: Se relacionan los riesgos como están definidos en la matriz de riesgos de SPI publicada en la matriz de riesgos institucional, la cual tiene fecha de aprobación agosto de 2021.* *- Pérdida de disponibilidad de la información del proceso por fallas en sistemas de información, aplicaciones, repositorios de información o servidores. Afectación a SIAD.* *- Pérdida de disponibilidad de la información de la entidad, los vigilados y/o usuarios finales. Afectación SIAD.* *- Pérdida de disponibilidad de la información contenida en los aplicativos de Gestión y sistemas de información. Afectación a los sistemas evaluados en esta auditoría y otros que no*	*"Los informes existentes fueron cargados en el repositorio de control interno* *Se restableció la información del sistema SIAD a corte 2016, y se realizaron varias actividades para reconstruir la información mediante sharepoit, archivos de Excel los cuales fueron dispuestos para el área* *Los sistemas de información presentaron indisponibilidad de servicio, y a partir del 22 de febrero fueron se restablecieron de manera paulatina hasta entregar todos sistemas operativos nuevamente, a excepción del sistema Siad que fue habilitado hasta la vigencia 2016, Las fuentes externas de analítica fueron restablecidas por parte del funcionario a cargo en la DID, la página web fue habilitada nuevamente luego de la migración de versión.*	El auditor de la Oficina de Control Interno verificó la información aportada por la DID/STI de las actividades desarrolladas por la DID y la STI para la atención de los incidentes de 2023. Al respecto, si bien se adelantaron actividades conducentes a la atención de los eventos, recuperación de los sistemas e infraestructura y, a tomar medidas para minimizar el impacto que generen nuevos ataques, se pudo evidenciar el incumplimiento de lo que define el Manual Para la Prestación del Servicio Para la Atención De Incidentes - DIMN13 en los siguientes aspectos: *"En la entrada del incidente; el registro, clasificación, Diagnostico, resolución y cierre del incidente. En cuanto el seguimiento y la Monitorización del Incidente."* La Oficina de Control Interno no evidenció la matriz de roles y responsabilidades de atención de incidentes tanto para la vigencia 2023 como del 1 de enero hasta el 30 de noviembre de 2024, además, no se evidenció que se documentara los incidentes del 17 de febrero de 2023 y 12 de septiembre de 2023 como también no se aportaron los soportes o evidencias de información detallada y técnica de este incidente por parte DID/STI. El auditor de la Oficina de Control Interno no evidenció los soportes de validación y análisis del incidente que fue catalogado como incidente mayor, en relación con la cantidad de usuarios afectados, la criticidad de los servicios afectados y su tiempo de afectación o caída de servicio afectando el principio de disponibilidad de la información. No se evidenció que se haya escalado el incidente de seguridad identificado como incidente mayor como lo establece la clave de éxito *"Gestionar TI"* y que direcciona a la clave de éxito *"Gestionar Problemas y Cambio"*. El auditor evidenció igualmente que la DID/STI no aportó documentación de lo que establece la actividad clave de éxito *"Gestionar Problemas y Cambios"* No se identificó la información relacionada con el incidente (actas de cambio, aceptación del área usuaria, etc.) para su respectivo registro en la base de datos de errores conocidos y su documentación en la base de datos de conocimiento. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno **Reitera la No Conformidad No. 1 Incumplimiento de Articulo 9 Gestión de incidentes de la resolución 00500 de**

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			fueron seleccionados en la muestra. *- Pérdida de integridad por destrucción o alteración de datos, programas o documentos electrónicos contenidos en aplicaciones o sistemas de información. Afectación a SIAD, base de datos de Analítica.* *- Pérdida de disponibilidad de la infraestructura tecnológica. Afectación a los sistemas evaluados en esta auditoría y otros que no fueron seleccionados en la muestra. Proveedor IFX Networks Colombia S.A.S.* *- Pérdida de confidencialidad por Fuga o robo de Información. Proveedor IFX Networks Colombia S.A.S.* *- Pérdida de la confidencialidad de aplicativos de gestión e infraestructura tecnológica. Proveedor IFX Networks Colombia S.A.S.* *- Pérdida de integridad por destrucción o alteración de datos, programas o documentos electrónicos contenidos en sistemas de información. Proveedor IFX Networks Colombia S.A.S.* *- Pérdida de integridad de la información respaldada o Backup. Proveedor IFX Networks Colombia S.A.S.* *Así mismo se evidencia la materialización de riesgos de gestión:* *- "Incumplimiento o Inadecuada implementación y mantenimiento en la adopción de los Estándares y Políticas de Modelo de Seguridad y Privacidad de la*	*Se precisa que la información fue encriptada Los sistemas de información presentaron indisponibilidad de servicio, y a partir del 22 de febrero se restablecieron de manera paulatina hasta entregar todos sistemas operativos nuevamente, a excepción del sistema Siad que fue habilitado hasta la vigencia 2016, Las fuentes externas de analítica fueron restablecidas por parte del funcionario a cargo en la DID, la página web fue habilitada nuevamente luego de la migración de versión."*	**2021** al proceso de *"Gobierno y Gestión de Datos e Información"* de la actividad *"Gestionar Problemas y Cambio"* liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno eleva no conformidad al proceso *"Gobierno y Gestion de Datos de Información"* - actividad clave de éxito *"Gestionar problemas y cambios"* liderado por la Dirección de innovación Desarrollo y al proceso *"Direccionamiento estratégico"* liderado por Oficina Asesora de Planeación, ante el incumplimiento preceptuado en el **Articulo 9 Gestión de incidentes de la resolución 00500 de 2021** al no gestionarse incidentes de seguridad y privacidad de la información con oportunidad, y calidad frente a la transferencia de conocimiento, Base de conocimiento (lecciones aprendidas), una adecuada gestión de riesgos, seguimiento y monitoreo a la gestión de incidentes y actualización de procedimientos definidos para atender dichos incidentes aspecto que resulta importante intervenir que permitirán manejar adecuadamente situaciones como las presentadas en 2023, logrando mitigar de manera acertada la materialización de riesgos, y con los cuales se podría generar una base de conocimientos para garantizar la integridad, confidencialidad, y la disponibilidad de los sistemas de información y de infraestructuras.

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			información", por la no aplicación adecuada de políticas de seguridad. - "Posibilidad de afectación reputacional por fallas en la operación de la Entidad, debido a la falta de cumplimiento de los Acuerdos de Nivel de Servicio (ANS) pactados", debilidad en la verificación de la gestión del proveedor de nube privada. - "Posibilidad de afectación económica y/o reputacional por hallazgo del ente regulador debido a la gestión y/o uso inadecuado de las herramientas de seguridad de la información existentes en la entidad", debilidad en los monitoreos"		

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
NO CONFORMIDAD	3	*"2.3.3 Incumplimiento a los lineamientos de la política del componente de seguridad de la información y seguridad digital contenida en el Manual de Políticas Institucionales, literal "c) La revisión de los riesgos de Seguridad de la Información y Seguridad Digital se llevará a cabo como mínimo una vez al año."*	*"En la verificación de Lineamientos de la Política del Componente de Seguridad de la Información y Seguridad Digital, el equipo auditor de la Oficina de Control Interno evidenció que no se está cumpliendo con este lineamiento, toda vez que, a la fecha de presentación de este informe, no se cuenta con la matriz de riesgos de seguridad y privacidad de la información actualizada.* *La última versión de la matriz publicada es de agosto de 2021 y en ella tampoco se evidencia que se haya realizado seguimiento a los controles definidos ni se registra si se han presentado materialización de riesgos.* *De otra parte, respecto del informe de monitoreo de riesgos de seguridad y privacidad de la información que emite semestralmente la STI, para la vigencia 2023 no se ha generado el correspondiente al primer semestre."*		El auditor de la Oficina de Control Interno realizará el respectivo análisis en el capítulo de riesgos del presente informe.
NO CONFORMIDAD	4	*"2.3.4 Incumplimiento a los lineamientos de las políticas del componente de seguridad de la información y seguridad digital para el control de accesos, en el ítem relacionado con "Gestión de contraseñas"*	*"El equipo auditor de la OCI evidenció que no se da cumplimiento al lineamiento de "Gestión de contraseñas" por lo que es pertinente que la STI implemente los controles necesarios para el registro de cambios de contraseñas "(…) cada vez que exista o haya algún indicio de una posible vulnerabilidad del sistema", en el que se registre la trazabilidad de las modificaciones efectuadas con la correspondiente explicación detallada de la realización de dichos cambios, acompañada de la respectiva matriz de riesgos de este y la*	*"Los cambios de contraseña están configurados de manera automática en el Directorio Activo y se corren cada 45 días esa información se presentó a control interno en la presentación."*	La Oficina de Control Interno evidenció debilidad en el cumplimiento a lo que define el lineamiento de la información en el manual FIMN07 *"Lineamientos de Política del Componente de Seguridad de la Información y Seguridad Digital"*, además, no se evidenció acto administrativo de la aprobación de las políticas de seguridad y privacidad de la información de la SNS, definidas en el manual FIMN07 y este no se encuentra en el listado maestro de documentos de la SNS. No se evidenció seguimiento a las políticas de seguridad y privacidad de la información de la SNS. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno se genera la **Recomendación N°. 3. Debilidad en la aprobación de las Políticas de Seguridad y privacidad de la Información**, al proceso *de "Gobierno y Gestión de Datos e Información" de la*

Seguimiento a las observaciones y no conformidades derivadas de la auditoría a sistemas de información realizada en la vigencia 2023					
TIPO DE HALLAZGO	**No.**	**TITULO**	**DESCRIPCION**	**Respuesta de DID / STI**	**Análisis de la Oficina de Control Interno**
			aprobación de la instancia pertinente en la STI; lo anterior en aras de conservar la base de conocimientos e históricos en los servicios, sistemas, servidores e infraestructura."		*actividad* ***clave de éxito*** *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: El auditor recomienda a la DID/STI que ponga a consideración las políticas de seguridad y privacidad de la información de la SNS al señor superintendente Nacional de Salud y al comité de Gestión y Desempeño Institucional para su aprobación.
NO CONFORMIDAD	5	*"2.3.5 Incumplimiento de las políticas del componente de Seguridad de la Información y Seguridad Digital "respaldo de la información".*	*"De acuerdo con la trazabilidad de este informe relacionada con los incidentes de seguridad presentados el 12/02/2023 y 17/02/2023, el equipo auditor de la OCI observó debilidad en el control que se debió ejercer por parte de la STI respecto del proveedor de servicios de nube privada, para verificar que estos controles se estuvieran ejecutando adecuadamente, lo que ocasionó la indisponibilidad de sistemas de información e infraestructuras, así como la pérdida de información del sistema SIAD, herramienta utilizada por la SDIA."*	*"Esta verificación fue ejercida por los supervisores de contrato"*	El auditor en la revisión de la documentación aportada sobre la realización de copias de seguridad, su tiempo de retención y del plan de recuperación de copias, solo evidencio la actualización del Manual para las copias de seguridad de la Información – DIMN14 donde solo se aplicó al Proceso de restauración 2024 al aplicativo **Sivica**l del 14 de agosto de 2024 y no se aportó las acciones y lineamientos definido en el manual para todas las aplicaciones con su respectiva documentación y plan de recuperación . Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno R**eitera la Recomendación N°. 2. Debilidad en la aplicación del Manual para las copias de seguridad de la Información – DIMN14**, al proceso de *"Gobierno y Gestión de Datos e Información"* en la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: la Oficina de Control Interno considera pertinente y necesario que la DID/STI cree una base de conocimiento y con su respectiva transferencia de conocimientos Así mismo, estos procedimientos permitirán detectar fallas oportunamente para tomar acciones de control y seguimiento con el fin de evitar la materialización de riesgos, que involucren la afectación de seguridad, integridad, y disponibilidad de la información.

1.2 Sistemas de información

Como parte de las acciones que se derivan del ejercicio auditor al *"Proceso Gobierno y Gestión de Datos e Información"*, las actividades claves de éxito *"Gestionar Seguridad y Privacidad de los Datos e Información"* y *"Gestionar aplicaciones"* que se viene adelantando con la Dirección de Innovación y Desarrollo y la Subdirección de Tecnologías de la Información de la Superintendencia Nacional de

Salud, dentro de la muestra alcance de la presente auditoria se seleccionó la Pagina Web, Gaudi; Sivical y Génesis de la Superintendencia Nacional de Salud, que hacen parte de la Actividad Clave de éxito *"Gestionar Aplicaciones"* que hacen parte del proceso Gobierno y Gestión de Datos e Información liderado por la Dirección de Innovación y Desarrollo, donde igualmente se solicitó la gestión realizada para dar cumplimiento de la Resolución 1519 de 2020 "*Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos*".

Metodología

Para verificación de la operatividad y funcionalidad de los Sistemas de Información, se seleccionó muestreo aleatorio simple de cuatro (4) sistema de información de catorce (14) del total de aplicativos y sistemas que se encuentran en producción en la Superintendencia Nacional de Salud, teniendo en cuenta los sistemas de información misionales, de apoyo y el grado de criticidad para la Entidad. El cuadro que se muestra a continuación contiene la base de 14 sistemas de información

No	Abreviatura	Nombre Aplicación Selección
1	NRVCC	Nuevo Sistema de Recepción y validación de archivos
2	SIAD	Sistema de Investigaciones Administrativas
3	ITS - GESTIÓN	Sistema Integrado de Planeación y Gestión
4	HUMANO®	Sistema de Gestión de Talento Humano y Nomina
5	FENIX	Sistema de Gestión y Control de las Medidas Especiales
6	RILCO	Sistema de Registro de Interventores, Liquidadores y Contralores
7	APLICA	Aplicativo para el Control de Activos
8	PQRD	Sistema para la Gestión de Peticiones, Quejas, Reclamos y Denuncias
9	Página Web	Página Web Institucional
10	INTRANET	Intranet Corporativa
11	CA	Service Desk Manager - mesa de servicios
12	GAUDI	Sistema de información para la ejecución de las funciones de Inspección, Vigilancia y Control de la SNS
13	GENESIS	Génesis es controlar el recaudo por concepto de tasa, régimen subsidiado, contribución y Sanciones
14	SIVICAL	Solución Informática para la Vigilancia, Inspección y Control de las apuestas en línea y tiempo real

Fuente: Oficina de Control Interno

Los cuatro sistemas de información que hicieron parte de la muestra son: Pagina Web, Gaudi, Genesis y Sivical.

Página web

La página web contiene documentos y enlaces (o hipervínculos o links) en los que se puede navegar entre contenidos, que contienen además *"colecciones de sitios"* que proporcionan una forma de agrupar los sitios web de manera que compartan una serie de características comunes, que

contienen una serie de configuraciones y cambios globales que se propagan desde el sitio raíz a todos los sitios que forman parte de la colección.

De acuerdo con el Decreto 1080 de 2021, la página esta descentralizada, es decir que el proceso que anteriormente se denominaba *"Comunicación Integral"* liderado por la Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional ahora está incluido como una actividad clave de éxito dentro del proceso *"Gobierno y Gestión de Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo.

Dentro de las actividades de los administradores de la página web se encuentra garantizar que se cumpla con las normativas vigentes, para lo cual dentro de esta verificación se observó que los lineamientos al interior de la entidad están formalizados a través del "*Manual para Publicación de Contenido en el Sitio Web de la Superintendencia Nacional de Salud"* - DIMN07, actualmente versión 3 del 19/01/2024.

Por lo anterior, se verificó el cumplimiento de lo exigido en las siguientes disposiciones:

- Resolución 1519 de 2020 en la cual establecen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución 2893 de 2020 que contiene los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado colombiano.
- Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
- ITA- Índice de Transparencia y Acceso a la Información Pública
- Ley 2345 de 2023 por la cual se implementa el manual de identidad visual de las entidades estatales, se prohíben las marcas de gobierno.

En la verificación efectuada respecto del cumplimiento de la Ley 2345 de 2023, se observó que al interior de la Entidad se emitió la campaña denominada *"Chao Marcas"*, para lo cual se hizo navegación por diferentes páginas internas, observando que algunos logos aún no se han actualizado en su totalidad, aspecto que fue socializado en prueba de recorrido del 24/09/2024; por lo expuesto la Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional informó que la solicitud de dicha actualización fue reportada a la Subdirección de Tecnologías de la Información mediante correo electrónico del 21/06/2024 tanto en las páginas del portal como de los logos en los diferentes aplicativos.

El Auditor de la Oficina de Control Interno evidenció una debilidad en el cumplimiento del Artículo 1 de la Ley 2345 de 2023 que tiene como objeto *"(…) establecer medidas que permitan unificar la imagen de las entidades estatales a través de la implementación del Manual de Identidad Visual, prohibiendo las*

marcas de gobierno con el fin de impedir que se pierda la identidad institucional, además de establecer medidas que permitan la austeridad en la publicidad estatal".

En relación con este tema, la Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional y la Subdirección de Tecnologías de la Información informaron que el trámite sigue en curso, dado que, para la actualización de aplicativos se realiza a través de proveedores, por lo que la Oficina de Control Interno recomienda continuar con la actividad hasta dejar unificados los logos con la nueva imagen en todos los sistemas de información de la entidad.

Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **Recomendación N°. 4. Debilidad en el Cumplimiento del Artículo 1 de la Ley 2345 de 2023** al proceso *"Gobierno y Gestión de Datos e Información",* en su actividad clave de éxito *"Gestionar Comunicaciones"* liderado por la DID y Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional así:

La Oficina de Control Interno recomienda continuar con la actividad hasta dejar unificados los logos con la nueva imagen en todos los sistemas de información de la entidad.

Genesis

La verificación del sistema de información de Génesis se realizó en la prueba de recorrido del 27 de septiembre 2024, de acuerdo con el cronograma de actividades definido para la ejecución de la presente auditoría. Por lo tanto, las novedades que se hayan presentado a partir de esas fechas no fueron verificadas en la presente auditoría.

Objetivo del Sistema

El objetivo del sistema de información Génesis es controlar el recaudo por concepto de tasa, régimen subsidiado, contribución y Sanciones, la creación y control de la cartera de esos procesos. En este sistema se crean los procesos, la sanción, la tasa adicional la contribución, la contribución adicional, la sanción, también permite hacer el proceso para que la entidad vigilada pueda pagar por código de barras o PSE.

Genesis surge como respuesta a la necesidad de actualización tecnológica para organizar e integrar todas las áreas funcionales y sus procesos, rompiendo el paradigma de sistemas monolíticos especializados por áreas al cambiar a un sistema modular por necesidades transversales de la entidad, considerando arquitecturas de solución orientadas a microservicios y gobierno del dato, permitiendo así la integración de funcionalidades por procesos y gestionar el conocimiento que se tiene sobre la información de la entidad.

La arquitectura de solución Génesis se basa en servicios del ecosistema Azure, en donde varios componentes funcionales se agrupan por módulos, y se exponen a través de servicios REST API, estos se conectan a una base de datos SQL Server en Azure y al mismo tiempo son consumidos por un Front End (Cliente Web .Net Core o del lado del cliente).

Durante las entrevistas a nivel técnico a la STI se informó que: *"El sistema de información es propio de la SNS, está desarrollado en Net Cord por varios ingenieros de desarrollo utilizando las herramientas que*

constituyen el Azure, los tres ambientes están en Azure tanto el desarrollo QA como producción bases de datos y producción, los servicios están sobre Azure."

Se tiene Loguin de cada uno de los usuarios bajo servicio Azure- Contrato con Microsoft, con almacenamiento en la nube Azure.

Accesos al sistema de Información

Roles y Perfiles

Para validar los funcionarios con acceso al sistema de información se solicitó a la STI el reporte del sistema de los roles, perfiles y usuarios activos del sistema de información, para lo cual el sistema cuenta con 17 roles debidamente descrito, en que consiste cada rol y el número de usuarios Activos en el sistema de información Genesis

No	Roles	Descripción	No. Usuarios
1	Admin	Tiene acceso a todos los módulos del sistema Genesis.	4
2	Consulta Contribución	Este rol permite visualizar informes del módulo de contribución.	11
3	Consulta Financiero	Este rol permite visualizar informes del módulo de Financiero.	18
4	Vigilado	Este rol es el que se le asigna a un usuario de una entidad vigilada.	
5	Liquidaciones Adicionales	Este rol permite gestionar y visualizar la liquidación de tasas adicionales.	7
6	Dirección EON	Este rol permite visualizar informes de contribución de esa dirección, así como el cargue de IOSC de fuente externa.	5
7	Mesa de Servicios	Este es para los agentes de mesa de servicios.	35
8	Dirección IPSS	Este rol permite visualizar informes de contribución de esa dirección, así como el cargue de IOSC de fuente externa.	6
9	Dirección EOT	Este rol permite visualizar informes de contribución de esa dirección, así como el cargue de IOSC de fuente externa.	13
10	Administrador Institucional	Este rol es para quien haga las veces de líder funcional	1
11	Administrador Financiero	Este rol permite tener acceso a informes y funcionalidades de cancelación, anulación y cargue de pagos.	6
12	Administrador Contribución	Este rol puede ver todas funcionalidades del módulo de contribución y aplicar la tarifa a las liquidaciones de contribución.	5
13	Seguridad	Este rol permite otorgar permisos a usuarios según el rol que se deba dar a cada uno.	1
14	Dirección EAPB	Este rol permite visualizar informes de contribución de esa dirección, así como el cargue de IOSC de fuente externa.	8
16	Consulta Cobro	Este rol permite visualizar informes del módulo de Financiero y contribución.	21
17	Gestor Jurisdiccional	Permite crear, administrar el módulo de Jurisdiccional.	21

Tabla 2 - Fuente oficina de control interno

La Oficina de Control Interno procedió a validar la asignación de usuarios según los tipos de roles definidos observando lo siguiente: para el sistema de información **Genesis** se encontró que hay 1

funcionario definido como administrador del sistema los cuales según el dato suministrado por la STI, la descripción del rol *"Tiene acceso todos los módulos del sistema Génesis"*, se identificaron 5 usuarios de la Dirección de Financiera y 1 usuario de la Subdirección de Tecnologías de la Información como **Administrador financiero**, *"Este rol permite tener acceso a informes y funcionalidades de cancelación, anulación, cargue de pagos"*, se identificaron 4 usuarios de la Dirección de Financiera y 1 usuario de la Subdirección de Tecnología de la información con el rol de **Administrador de Contribución** *"Este rol puede ver todas funcionalidades del módulo de contribución y aplicar la tarifa a las liquidaciones de contribución"*; se identificaron 16 usuarios de la Dirección de Financiera, 1 usuario de la Subdirección de Tecnología de la Información y 1 usuario de la Contraloría para **Consulta Financiero**, "*Este rol permite visualizar informes del módulo de Financiero*", para este se identificó a 10 usuarios de Dirección Financiera y 1 usuarios del Subdirección de Tecnología de la Información para **Consulta Contribución** *"Este rol permite visualizar informes del módulo de contribución", ver tabla 1*

El rol para módulo de Seguridad este asignado a un funcionario de la subdirección de Tecnología de la información *"Este rol permite otorgar permisos a usuarios según el rol que se deba dar a cada uno"* el cual es el encargado de asignar los roles y permisos a todos los funcionarios activos de las áreas funcionales y de la Subdirección de Tecnología de la información "*en cuanto soporte, parametrización, desarrollos nuevos del Sistema de información* ***Genesis*****"**.

Gaudi

La verificación de sistema de información de **Gaudi** se realizó de acuerdo con el cronograma de actividades definido para la ejecución de la presente auditoría. Por lo tanto, las novedades que se hayan presentado a partir de esas fechas no fueron verificadas en la presente auditoría.

Objetivo del Sistema

En sistema de información dispuesto por la SNS para Guiar la auditoría como estrategia para cumplir las funciones de inspección y vigilancia de las entidades territoriales en relación con las responsabilidades y obligaciones del aseguramiento y prestación de servicios de salud a cargo de las empresas promotoras de salud habilitadas en las jurisdicciones territoriales.

Usuarios activos		
Nombre del Rol	**No. Usuarios Funcionales**	**No. Usuarios Técnico**
Administrador Configuración	0	0
Administrador Datos Generales	0	0
Administrador Funcional	0	0
Administrador Gaudi	4	1
Administrador Retransmisiones	0	0
Administrador Seguridad	0	0
Auditor Gaudi	2	1

Usuarios activos		
Nombre del Rol	**No. Usuarios Funcionales**	**No. Usuarios Técnico**
Consulta	17	3
Personal Funcional Del Vigilado	2	1
Representante Legal	0	0
Retransmisión [Demo]	0	0
Trámites	0	3
Verificador Gaudi	14	1

Tabla 2 Fuente: Oficina de control Interno

En el sistema **Gaudi**, se identificaron 2 usuarios internos del áreas misionales y 1 del área de tecnología con el rol de **Auditor Gaudi**, se tienen 4 usuarios de la Delgada de entidades territoriales y 1 usuarios de la Subdirección de Tecnologías de la Información; como **Administrador Gaudi**, se identificaron 17 usuarios de Delegada de entidades territoriales y 2 usuarios del Subdirección de Tecnología de la Información, 1 usuario de la Oficina de Control Interno con el Rol de **Consulta**, se identificaron 14 usuarios de la Delegada de entidades territoriales, 1 usuarios del Subdirección de Tecnología de la Información para **Verificador Gaudi.**

Usuarios Inactivos		
Nombre del Rol	**No. Usuarios Funcional**	**No. Usuarios Técnico**
Administrador Configuración	3	12
Administrador Datos Generales	0	4
Administrador Funcional	4	12
Administrador Gaudi	14	4
Administrador Retransmisiones	2	1
Administrador Seguridad	2	12
Auditor Gaudi	24	3
Consulta	21	1
Personal Funcional Del Vigilado	2	1
Trámites	3	1
Verificador Gaudi	34	3

Fuente: elaborado por la Oficina de Control Interno

El Auditor de la Oficina de Control Interno evidenció que existen Roles con estado Inactivo como lo son: **Administrador Configuración** con 3 funcionarios de las áreas funcionales y 12 del área técnica, **Administrador Datos Generales** con 0 funcionarios del área funcional y 4 del área técnica, Administrador Funcional 4 usuarios de las áreas funcionales y 12 del área técnica, **Administrador Gaudi**, con 14 usuarios de las áreas funcionales y 4 usuarios del área técnica, **Administrador Retransmisiones** con 2 usuarios de las áreas funcionales y 1 del área técnica, **Administrador**

Seguridad con 2 usuarios de las áreas funcionales y 12 usuarios del área técnica, **Auditor Gaudi** con 24 usuarios de las áreas funcionales y 3 del área técnica, **Consulta** con 21 usuarios de las áreas funcionales y 1 del área técnica, **Verificador Gaudi** con 34 usuarios de las áreas funcionales y 3 del área técnica con estado **inactivo**, y en algunos casos se observó usuarios que no están vinculados de manera contractual o laboral a la fecha de la presente auditoria.

Conforme la información aportada por la STI el Auditor evidenció que en la base de datos de usuarios interno con estado inactivo hay usuarios con correos electrónicos no institucionales, lo que describe que no se realizó la validación de usuarios contra directorio activo de la SNS.

En el rol para módulo de Seguridad está asignado a un funcionario de la Subdirección de Tecnologías de la Información, *"Este rol permite otorgar permisos a usuarios según el rol que se deba dar a cada uno"* el cual es el encargado de asignar los roles y permisos a todos los funcionarios activos de las áreas funcionales y de la Subdirección de Tecnología de la información *"en cuanto soporte, parametrización, desarrollos nuevos del Sistema de información* ***Genesis***".

Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera **Observación N°. 5. Debilidad en la definición de Roles y Responsabilidad por falta de segregación de funciones en los Sistemas de Información Génesis y Gaudi** al proceso *"Gobierno y Gestión de Datos e Información"* actividad clave de éxito *"Gestionar Aplicaciones"***, liderado** por la Dirección de Innovación y Desarrollo (en adelante DID), así:

La Oficina de Control Interno evidenció que los usuarios con acceso a los sistemas de información frente a los roles y responsabilidades establecidos en **Génesis, Sivical, y Gaudi**, sobre los cuales se identificaron usuarios asociados tanto a lo funcional como a lo técnico, lo cual estaría generando limitación en las transacciones, las cuales deben tener acceso acorde a sus funciones y responsabilidades, de forma que se mitiguen riesgos al hacer una adecuada segregación de funciones

La Oficina de Control Interno considera pertinente se reevalúe en todos los sistemas de información y se establezcan los roles y responsabilidades, de tal forma que se tenga a nivel de la entidad una adecuada segregación de funciones, lo cual garantiza una administración segura y eficaz para las actividades que desarrollan los funcionarios de las áreas funcionales y de la DID/STI**.**

Sivical

Objetivo

El Sistema de Inspección y Vigilancia de Apuestas en Línea - SIVICAL, se encarga de recibir la información en línea y tiempo real de los datos provenientes de juegos de apuestas permanentes o chance del territorio nacional.

En las mesas de trabajo y prueba de recorrido al sistema de información SIVICAL por parte del auditor de la OCI se observó lo siguiente:

Generalidades

SIVICAL recibe diferentes tipos de insumos de información mediante la plataforma Génesis o utilizando el envío de tramas en la APP diseñada en Azure.

En la plataforma génesis se reciben tres tipos de archivos:

- Vendedores: Archivo .CSV, información que alimenta la tabla de referencia de vendedores, conteniendo los datos básicos de las personas que han sido contratadas para realizar las ventas de los juegos de azar.
- Máquinas: Archivo .CSV, información que alimenta la tabla de referencia Máquinas, conteniendo la data que permite identificar las maquinarias que cada concesionario tiene
- Incentivos: Archivo .CSV, información que alimenta la tabla de referencia incentivos, conteniendo la data de los incentivos que han sido otorgados a cada uno de los concesionarios.

También se evidenció que en la APP se reciben dos tipos de archivos:

- Trama de inserción: información clasificada como tipo 1, que contiene los datos de la apuesta (número y valor apostado), el municipio, máquinas y vendedor.
- Trama de anulación: Información clasificada como tipo 2, contiene los datos que permiten realizar la anulación de las tramas enviadas.

Por último, el auditor de la Oficina de Control Interno evidenció que toda la información remitida bien sea por Génesis o por la APP de SIVICAL es insertada en el servidor Azure dispuesto para tal fin en la base de datos SIVICAL.

REPORTES

Existen dos tipos de reportes generados con la información almacenada en SIVICAL, un grupo orientado a los funcionarios de la superintendencia Nacional de Salud y otro grupo orientado a los concesionarios.

Al revisar los reportes externos se tienen cuatro diseñados:

Imagen 1 fuente: Subdirección de Tecnología de la Información

ROLES

SIVICAL tiene dos tipos de roles, asociados al sistema que permite la carga de información (tramas) o al usuario creado en el sistema GENESIS:

Se evidenciaron los siguientes roles creados mediante la aplicación GENESIS:

- **Rol SIVICAL**: Permite a los concesionarios el cargue de archivos (máquinas, vendedores e incentivos) y la consulta de los reportes.
- **SNS SIVICAL**: Permite únicamente a los funcionarios de la SNS el ingreso a los reportes de consulta.

Rol de SIVICAL en la APP

Existe un solo rol en la APP que es el ejercido por el concesionario, para esto el concesionario debe estar activo tanto en génesis como autorizado para el consumo del servicio B2C.

El auditor de la OCI, en las pruebas de recorrido en sitio observó que, en los servidores alojados en Azure, los cuales están dispuestos para el almacenamiento de las transacciones en producción y consulta donde se consumen en almacenamiento 26 GB diarias y 800 GB mensuales y con un acumulado anual de 9.8 TB, aunado a esta situación, la herramienta que se utiliza para el almacenamiento es Microsoft Azure es un servicio que tiene un alto costo y que se puede ver reflejado en el manejo de la APP

Así mismo el auditor evidenció que el número de transacciones es muy alto, lo que conlleva a que la generación de reportes relacionados en la **imagen 1** sea bastante lento aproximadamente una hora o más por cada reporte.

También se evidenció que falta ajustar y completar los documentos que se relacionan con la infraestructura, bases de datos y funcionamiento como manuales en algunos casos no se encuentran aprobados y en los formatos autorizados por la Oficina Asesora de Planeación.

Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **Recomendación 5. Debilidad en la generación de reportes del Sistema de información**

SIVICAL al proceso *"Gobierno y Gestión de Datos e Información"* en la actividad clave de éxito *"Gestión de Aplicaciones"***,** liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así**:**

El auditor de la Oficina de Control Interno, a partir de la información recaudada, recomienda al líder del proceso *"Gobierno y Gestión de Datos e Información"*, vale decir, Dirección de Innovación y Desarrollo y a la Subdirección de Tecnología de la Información que se Optimice el almacenamiento de información de las transacciones que se encuentran en los servidores alojados en Azure (Producción y consulta) del sistema de información SIVICAL, con ello se disminuyan los costos en el manejo de la APP.

Así mismo que se realicen los desarrollos o ajuste necesarios para la optimización de la generación de los reportes generados a través del sistema de información SIVICAL, con ello se daría respuesta de manera oportuna y con calidad a las diferentes solicitudes de los Concesionarios.

1.3 Seguridad y Privacidad de los Sistemas de Información

Se precisa que, en actividad de seguimiento efectuada por la Oficina de control Interno a la Ley 1712 de 2014 - ITA "*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*", para el periodo comprendido entre el 01 de septiembre de 2023 al 30 de agosto de 2024, se realizó el análisis y evaluación respecto del anexo 1 *"Directrices de accesibilidad web"* y, Anexo 2 "*Estándares de publicación y divulgación información*", razón por la cual, no hacen parte de la presente auditoría, en el entendido que, estas situaciones ya fueron evaluadas, de lo cual se plasmaron los resultados del seguimiento en el citado informe que se encuentra dispuesto para consulta de las partes interesadas a través del siguiente enlace:

https://docs.supersalud.gov.co/PortalWeb/ControlInterno/InformesEstatutoAnticorrupcion/SS%20%20Seg%20ITA%202024140000009781 3%2030-09-2024.pdf

Aunado a lo anterior, en el numeral dos (2) del citado informe de seguimiento, se relacionan los resultados obtenidos, esto es, los hallazgos "*Conformidad*", *"Observaciones"* y *"No Conformidades"*, así como, las *"Recomendaciones"* derivadas del ejercicio realizado por la Oficina de Control Interno.

Así las cosas, el presente informe abarca el análisis y evaluación del cumplimiento del Anexo 3 *"Condiciones mínimas técnicas y de seguridad digital"*.

Por lo expuesto, el auditor realizó verificación del cumplimiento del anexo 3 del Artículo 6. *"Condiciones mínimas técnicas y de seguridad digital. Los sujetos obligados deberán observar las condiciones mínimas técnicas y de seguridad digital que se definen en el Anexo 3 de la presente resolución"*. De la Resolución 1519 de 2020 *"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"*.

El Auditor de la Oficina de Control Interno realizó solicitud de información a través de memorando con radicado 20241400000091973 del 11 de septiembre de 2024 enviado a la jefe de la Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional, líder de la actividad clave de éxito *"Gestionar las Comunicaciones"* y se compulsó copia a la Dirección de innovación y Desarrollo y a la Subdirección de Tecnología

De acuerdo con lo definido en el plan de auditoría, uno de los ítems verificados fue el sitio Web www.supersalud.gov.co que hace parte de la actividad clave de éxito *"Gestionar Comunicaciones"* que lidera la Oficina Asesora de Comunicaciones Estratégicas y de las aplicaciones: SIVICAL, Genesis y Gaudi de la Superintendencia Nacional de Salud, las actividades claves de éxito *"Gestionar Seguridad y Privacidad de los Datos e Información"* y *"Gestionar Aplicaciones"* y cuyo líder del proceso *"Gobierno de Gestión de Datos e Información"* es la Dirección de innovación y Desarrollo, se validaron los aspectos relacionados con seguridad, confidencialidad, integridad y disponibilidad de los sistemas de información seleccionados, cuyo resultado se expone a continuación.

Anexo 3 - Condiciones mínimas técnicas y de seguridad digital:

"3.1 DEFINICIONES GENERALES.

Definiciones generales aplicables al presente anexo:

1. Cookies: Archivo creado por los sitios web en donde se almacenan datos sobre la navegación del usuario.
2. colCERT: Grupo de Respuesta a Emergencias Cibernéticas del Ministerio de Defensa Nacional.
3. CSIRT – Gobierno: Grupo de Respuestas a Incidentes de Seguridad Informática del Gobierno Nacional.
4. Defacement: Denominación en inglés que hace referencia al tipo de ataque cibernético, bajo el cual, se desconfiguran los contenidos del sitio o portal web, incluso poniéndoles "otra cara" mediante colores, imágenes o contenidos no originales.
5. Escape de variables en el código: Proceso de validación para confirmar que los datos ingresados en una variable correspondan con las entradas o caracteres válidos asignados por defecto en su configuración.
6. Hardening: En el contexto de seguridad digital, hardening o endurecimiento, implica eliminar todas las configuraciones por defecto, reduciendo las vulnerabilidades y asegurando los sistemas e infraestructuras digitales.
7. Plugins: Herramientas o aplicaciones de software que realizan funciones específicas, añadiendo en un software principal.
8. Políticas de origen de las cabeceras: Serie de reglas que garantizan la seguridad de las cabeceras del protocolo HTTP.
9. Script. Es un conjunto de comandos que se usa para la configuración del código fuente.
10. Token de CSRF: Código único de seguridad enviado en forma remota para validar la identidad del usuario.

3.2 CONDICIONES DE SEGURIDAD DIGITAL

Los sujetos obligados tendrán que adoptar medidas para garantizar la seguridad digital y mitigar riesgos de incidentes cibernéticos o filtración de datos personales o sensibles, observando lo siguiente:

1. Adoptar autónomamente políticas para implementar un sistema de gestión de seguridad digital y de seguridad de la información, conforme con las buenas prácticas internacionales. Entre otros podrán implementar los estándares de la familia ISO 27000 y/o los recomendados por el Instituto Nacional de Tecnología y Estándares (NIST, por sus siglas en inglés). Para cumplimiento de lo anterior se requiere la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) recomendado por la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

2. Las entidades públicas del orden nacional y territorial, en caso de incidentes cibernéticos graves o muy graves, conforme con los criterios de su sistema de gestión de seguridad digital y seguridad de la información, deberán reportarlos por tardar dentro de las 24 horas siguientes a su detención al CSIRT-Gobierno. Para el resto de los sujetos obligados, deberán reportar al ColCERT del Ministerio de Defensa Nacional."

El auditor verificó el cumplimiento del Anexo 3 de la resolucion1519 2020 con las evidencias y soportes aportados por la DID/STI se encontró lo siguiente:

Anexo 3 - Análisis OCI - Condiciones mínimas técnicas y de seguridad digital				
Nivel	**Contenido**	**Lineamiento**	**Justificación Cumplimiento**	**Análisis OCI**
3.2	*"Condiciones de seguridad digital"*	*"Adoptar autónomamente políticas para implementar un sistema de gestión de seguridad digital y de seguridad de la información, conforme con las buenas prácticas internacionales. Entre otros podrán implementar los estándares de la familia ISO 27000 y/o los recomendados por el Instituto Nacional de Tecnología y Estándares (NIST, por sus siglas en inglés). Para cumplimiento de lo anterior se requiere la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) recomendado por la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones."*	Durante el periodo a reportar se ejecutaron diferentes actividades que llevan a que en un futuro se pueda implementar totalmente el Modelo de Seguridad y Privacidad de la Información – MSPI, no obstante, se realizó el contrato con la corporación Colombia Digital para dar inicio a diferentes acciones encaminadas a implementar completamente el modelo.	La Oficina de Control Interno evidenció lo siguiente: No se aportó el acto administrativo de la aprobación de las políticas de seguridad y privacidad de la información de la SNS, definidas en el manual FIMN07 *"Lineamientos de Política del Componente de Seguridad de la Información y Seguridad Digital"* y este no se encuentra en el listado maestro de documentos de la SNS No se evidenció seguimiento a las políticas de seguridad y privacidad de la información de la SNS. El cumplimiento del diligenciamiento del instrumento del estado de madurez del MSPI de la entidad, se encuentra en un grado de madurez del 33% del 100 que sígnica que está por debajo del indicador aceptado para el cumplimiento de valoración del MSPI para el 2024 Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno **genera Observación N°. 6. Debilidad en cumplimiento de anexo 3 de la resolución 1519 de 2020** al proceso *"Gobierno y Gestión de Datos e Información"* en la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"* y *"Gestión de Aplicaciones"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así:

Anexo 3 - Análisis OCI - Condiciones mínimas técnicas y de seguridad digital				
Nivel	**Contenido**	**Lineamiento**	**Justificación Cumplimiento**	**Análisis OCI**
				La Oficina de Control Interno insta a la DID/STI de manera prioritaria a que se tomen las acciones necesarias para que el indicador de evaluación del estado de madurez del sistema de gestión de seguridad de la información este por encima del 60% conforme los establece la resolución 00500 de 2021 de MINTIC.
3.2.1	*"Controles en el desarrollo de sitios web y aplicaciones"*	*"Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software"*	La entidad a través del PETI 2024 describe el proceso de Gestión y desarrollo de software. La Gestión y Desarrollo de Software abarca el ciclo de vida completo del desarrollo de software, desde la concepción y diseño hasta la implementación y mantenimiento. Involucra la gestión de proyectos, la colaboración entre equipos, y la adopción de metodologías como Agile, Scrum o DevOps para mejorar la entrega eficiente y la calidad del software.	El Auditor de la Oficina de Control Interno evidenció debilidad en el cumplimiento de los controles de seguridad y privacidad de la información implementados por la SNS en cuanto el ciclo de vida de desarrollo del sitio Web y de desarrollo, no se observó el diligenciamiento del formato *"REQUERIMIENTOS DE SEGURIDAD PARA APLICACIONES- DIFT25"* Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **Recomendación N°. 6. Debilidad en el cumplimiento del numeral 3.2.1 del anexo 3 de la resolución 1519 de 2020** al proceso de *"Gobierno y Gestión de Datos e Información"* en la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, *"Gestión de Aplicaciones"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno recomienda DID/STI se diligencie el formato *"Requerimientos de Seguridad Para Aplicaciones- DIFT25"* con el fin de aplicar buenas prácticas de desarrollo seguro.

Anexo 3 - Análisis OCI - Condiciones mínimas técnicas y de seguridad digital				
Nivel	**Contenido**	**Lineamiento**	**Justificación Cumplimiento**	**Análisis OCI**
3.2.4	*"Controles en el desarrollo de sitios web y aplicaciones"*	*"Aplicar mecanismos de hardening para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota."*	Página: Se Asegura de que la cuenta de administrador y la cuenta de invitado predeterminadas requieran una contraseña, enlazados con el A.DCHATBOTS: No aplica, porque están embebidos en la página de la Supersalud. La entidad a través del servicio de WAF (Web Application Firewall) que tiene desplegado en la nube de Azure, permite mitigar los riesgos asociados con métodos HTTP peligrosos como PUT, DELETE y TRACE, además los WAF están diseñados para inspeccionar y filtrar el tráfico web, bloqueando ataques antes de que lleguen a la aplicación.	El Auditor conforme la información aportada por DID/STI describen lo siguiente *"no es posible determinar los mecanismos específicos de hardening o endurecimiento que se han implementado para blindar el aplicativo y prevenir riesgos en seguridad. Desde el desarrollo de la aplicación no se identifican procesos de cargue de información por usuarios externos donde se pueda filtrar script malicioso."* Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno se formula la **Recomendación N°. 7. Debilidad en el cumplimiento del numeral 3.2.4 anexo 3 de la resolución 1519 de 2020** al proceso *"Gobierno y Gestión de Datos e Información"* de la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información", "Gestión de Aplicaciones"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno recomienda DID/STI Aplicar mecanismos de hardening para eliminar configuraciones y credenciales por defecto.

Anexo 3 - Análisis OCI - Condiciones mínimas técnicas y de seguridad digital				
Nivel	**Contenido**	**Lineamiento**	**Justificación Cumplimiento**	**Análisis OCI**
3.2.6	*"Controles en el desarrollo de sitios web y aplicaciones"*	*"Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios."*	El monitoreo y protección se realiza a través de Fortigate onpremise, Fortigate nube, FortiWeb, Fortisandbox, antivirus, la entidad no cuenta con una herramienta para escaneo de vulnerabilidades, pero se realizó análisis a los siguientes aplicaciones (paginaweb, intranet, genesis, nrvcc, SIVICAL y humano)	La Oficina de Control Interno de acuerdo con la información aportada observó lo siguiente: no se evidencian soportes de escaneo de archivos infectados, escaneo de vulnerabilidades de Gaudi, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicio de Gaudi, Sivical, Pagina WEB y Genesis. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **Observación N°. 7. Debilidad en el cumplimiento del numeral 3.2.6 anexo 3 de la resolución 1519 de 2020** al proceso de *"Gobierno y Gestión de Datos e Información"* en la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, *"Gestión de Aplicaciones"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno conmina a la DID/STI a que se tomen las acciones que correspondan para realizar de manera periódica el escaneo de archivos infectados, escaneo de vulnerabilidades de Gaudi análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicio de las aplicaciones activas de la SNS con el fin de detectar, prevenir y corregir afectaciones, materialización del riesgos de seguridad y privacidad de la información, para garantizar la disponibilidad, Integridad y confidencialidad de la información de la SNS.

Anexo 3 - Análisis OCI - Condiciones mínimas técnicas y de seguridad digital				
Nivel	**Contenido**	**Lineamiento**	**Justificación Cumplimiento**	**Análisis OCI**
3.2.16	*"Controles en el desarrollo de sitios web y aplicaciones"*	*"Proteger el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación."*	CHATBOTS: No aplica, los códigos se encuentran compilados, por lo cual no se puede acceder al código fuente. RILCO: No cumple - no se tiene conocimiento ni existe documento que conste que se ha realizado una protección Binaria del código NRVCC: No aplica porque no se cuenta con documentación para protección del binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing). Gaudi: No cumple - no se tienen conocimiento de documentación para protección del binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing). Fenix no cumple, pero no está al alcance del atacante para realizar algún tipo de ingeniería inversa. ya que se encuentra salvaguardado en Azure DevOps con su respectiva y robusta seguridad, de esta forma el atacante nunca tiene acceso al código fuente. El código de SIVICAL no está al alcance para realizar algún tipo de ingeniería inversa ya que se trata de transmisión de información por medio de tokens de seguridad, de esta forma el concesionario nunca tiene acceso a código fuente o una página a la cual le pueda realizar la revisión de la lógica.	El Auditor de la Oficina de Control Interno de acuerdo con la información aportada observó lo siguiente: no evidenció soportes de proteger el binario de las algunas aplicaciones, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno **Reitera la observación N°. 7 Debilidad en el cumplimiento del numeral 3.2.6 anexo 3 de la resolución 1519 de 2020** al proceso *"Gobierno y Gestión de Datos e Información"* de la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, *"Gestión de Aplicaciones"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno recomienda a la DID/STI a que se proteja el binario de las aplicaciones Rilco, nRVCC entre otras, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) que eviten analizar la lógica de la aplicación.

Anexo 3 - Análisis OCI - Condiciones mínimas técnicas y de seguridad digital				
Nivel	**Contenido**	**Lineamiento**	**Justificación Cumplimiento**	**Análisis OCI**
3.2.20	*"Controles en el desarrollo de sitios web y aplicaciones"*	*"Implementar en los servidores los controles necesarios (hardware o software) de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros."*	En la entidad se encuentra instalado en los diferentes servidores instalado el antivirus institucional y a nivel perimetral con el WAF. PQRS: El framework laravel ya se tiene incluida la protección contra sql injection, X-XSS-Protection se encuentra habilitado por defecto en los navegadores actuales para prevenir el cross site scripting. https://cheatsheetseries.owasp.org/cheatsheets/Laravel_Cheat_Sheet.html#sql-injection. superargo con la librería adodb por medio de bind variables: https://adodb.org/dokuwiki/doku.php?id=v5:userguide:learn_bind:bind_vars	La Oficina de Control Interno de acuerdo con la información aportada observó lo siguiente: no evidenció que se haya realizado análisis de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros, de las aplicaciones objeto de la Muestra página web, Genesis, Gaudi y Sivical, se realizó análisis de vulnerabilidad del 24 al 28 de febrero y en agosto de 2024 y sobre ninguna se evidenció la realización del análisis de vulnerabilidades a las aplicaciones de la muestra. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **Observación N°. 8. Debilidad en el cumplimiento del numeral 3.2.20 anexo 3 de la resolución 1519 de 2020** al proceso de *"Gobierno y Gestión de Datos e Información"* en la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, *"Gestión de Aplicaciones"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno recomienda a la DID/STI a que se realice de manera periódica análisis de vulnerabilidades a todas las aplicaciones activas de la SNS.

Anexo 3 - Análisis OCI - Condiciones mínimas técnicas y de seguridad digital				
Nivel	**Contenido**	**Lineamiento**	**Justificación Cumplimiento**	**Análisis OCI**
3.2.22	*"Controles en el desarrollo de sitios web y aplicaciones"*	*"Implementar monitoreos de seguridad sobre la plataforma tecnológica que hace parte del sitio web (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes."*	El monitoreo y protección se realiza a través de Fortigate onpremise, Fortigate nube, FortiWeb, Fortisandbox, antivirus, la entidad no cuenta con una herramienta para escaneo de vulnerabilidades, pero se realizó análisis a las siguientes aplicaciones (paginaweb, intranet,genesis,nrvcc y sivical)	El Auditor de la Oficina de Control Interno de acuerdo a la información aportada no pudo dar cuenta del monitoreo de: escaneo de vulnerabilidades SIVICAL y Genesis, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios y realizar las acciones de mitigación correspondientes de las anteriores actividades referenciadas, además no se evidenciaron soportes. Así mismo, no se observó ninguna acción o remediación del análisis según recomendación hecha en el análisis de vulnerabilidades realizada del 15 al 16 agosto 2024 ver imagen 2. Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno formula la **Observación N° 9 Debilidad en el cumplimiento del numeral 3.2.22 del anexo 3 de la resolución 1519 de 2020** al proceso de *"Gobierno y Gestión de Datos e Información"* en la actividad *"Gestionar Seguridad y Privacidad de los Datos e Información"*, *"Gestión de Aplicaciones"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así: La Oficina de Control Interno conmina a la DID/STI a que se tomen las acciones que correspondan para realizar de manera periódica monitoreo de :escaneo de vulnerabilidades de las aplicaciones activas de la SNS, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios y realizar las acciones de mitigación correspondientes de las aplicaciones activas de la SNS con el fin de detectar, prevenir y corregir afectaciones, desviaciones, materialización del riesgos de seguridad y privacidad de la información, con el fin de garantizar la disponibilidad, Integridad y confidencialidad de la información de la SNS.

Anexo 3 - Análisis OCI - Condiciones mínimas técnicas y de seguridad digital				
Nivel	**Contenido**	**Lineamiento**	**Justificación Cumplimiento**	**Análisis OCI**
3.2.26	*"Controles en el desarrollo de sitios web y aplicaciones"*	*"Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web."*	La entidad tiene implementado un proceso para el escalamiento de privilegios. PQRD: Los servicios de web y base de datos son ejecutados con un usuario independiente, para los usuarios que requieren acceder a la base de datos se tiene limitado los privilegios. SuperArgo: Los servicios de web y base de datos son ejecutados con un usuario independiente, para los usuarios que requieren acceder a Página Web: la base de datos se tiene limitado los privilegios, El control de escalamiento de privilegios de las cuentas de usuarios se realiza a través del directorio activo y Azure Active Directory	Cumple.

1.4 Cumplimiento resolución 00500 de 2021

El Auditor de la Oficina de Control Interno realizó seguimiento al cumplimiento de la Resolución 00500 de 2021 de la SNS dentro del alcance de la presente auditoria. El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, como entidad encargada de diseñar, adoptar y promover políticas, planes, programas y proyectos en el uso y apropiación de las TIC, estableció lineamientos para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones TIC. Además, establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las Entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos.

Por lo anterior el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC expidió la Resolución 00500 de 2021 *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital",* cuyo objetivo está establecido en el Artículo 1 de la presente resolución, así: *"ARTÍCULO 1. Objeto. La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos*

de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital."

El auditor de la OCI, en el ámbito de la ejecución de la presente auditoria verificó el cumplimiento de cada de los artículos 3, 4, 5, 6, 9, 10,15 y 17 de la resolución 00500 de 2021, así:

"ARTÍCULO 3. Lineamientos generales. Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución. Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura critica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital."

Frente al cumplimiento de este artículo y conforme la información aportada por DID/STI el auditor evidenció lo siguiente:

Plan de Seguridad y Privacidad de la Información (2024) - www.supersalud.gov.co se encuentra publicado en el portal de la SNS, no fue objeto del alcance de la presente Auditoria.

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (2024), se evidenció que no se encuentra actualizado y aprobado para la vigencia 2024.

Frente a la adopción de los lineamientos del MSPI y los documentos aportados por DID/STI, la Oficina de Control Interno, verificó en el instrumento de evaluación de MSPI el avance de la Línea Base de Seguridad y se identificó los siguiente:

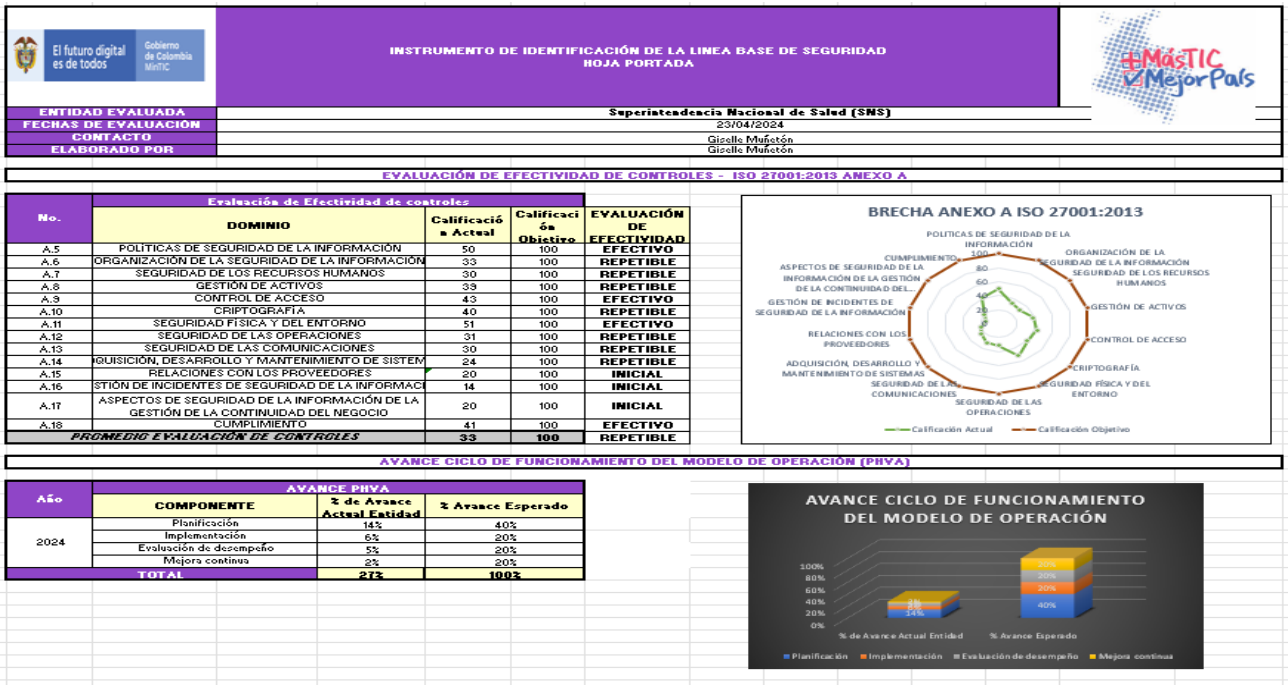
No se aportó el acto administrativo de la aprobación de las políticas de seguridad y privacidad de la información de la SNS que se encuentran contenidas en el Manual de Políticas Institucionales asociadas al Sistema Integrado de Gestión- SIG – DEFT13 y los Lineamientos de Política del Componente de Seguridad de la Información y Seguridad Digital – FIMN07, el cual no se encuentra en listado maestro de documentos de la Supersalud.

No se evidenció seguimiento a las políticas de seguridad y privacidad de la información de la SNS.

El cumplimiento del diligenciamiento del instrumento del estado de madurez del MSPI de la entidad, el auditor de la OCI verificó la evaluación de efectividad y eficacia de los controles -ISO 27001 de 2013 Anexo A, evidenciando que el porcentaje de cumplimiento es del 33% como se evidencia en la **imagen 2**, lo que significa que se encuentra en la escala de evaluación *"**Repetible**"* de 40%, por debajo del indicador aceptado para el cumplimiento de valoración del MSPI para el 2023 – 2024 y se denota debilidad en el cumplimiento de los lineamientos de la evaluación de MSPI por parte de

la SNS, aunado que la resolución fue expedida el 10 de marzo de 2021 y que a la fecha de la presente auditoria debería estar como mínimo en un 60 % de cumplimiento como se evidencia en la **imagen 3**:

Instrumento de Identificación de la Línea Base de Seguridad de la SNS



INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

ENTIDAD EVALUADA	Superintendencia Nacional de Salud (SNS)
FECHAS DE EVALUACIÓN	23/04/2024
CONTACTO	Giselle Muñoz
ELABORADO POR	Giselle Muñoz

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	33	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	30	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	39	100	REPETIBLE
A.9	CONTROL DE ACCESO	43	100	EFECTIVO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FISICA Y DEL ENTORNO	51	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	31	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	30	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEM	24	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACI	14	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	41	100	EFECTIVO
	PROMEDIO EVALUACIÓN DE CONTROLES	33	100	REPETIBLE

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	14%	40%
	Implementación	6%	20%
	Evaluación de desempeño	5%	20%
	Mejora continua	2%	20%
	TOTAL	27%	100%

Imagen 2. Fuente Subdirección de Tecnologías de la Información

El Auditor de la Oficina de Control Interno evidencia debilidad en el cumplimiento del Avance Ciclo de Funcionamiento del Modelo de Operación (PHAV) es del 27 % distribuido de la siguiente manera:

AVANCE PHVA – SNS

Año	Componente	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	14%	40%
	Implementación	6%	20%
	Evaluación de desempeño	5%	20%
	Mejora continua	2%	20%
	Total	**27%**	**100%**

Fuente: Oficina de control interno

Planificación: es la fase donde la entidad realiza la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI, en la SNS se encuentra en un 14% cuando el avance esperado es de 40%.

Implementación: es la fase que inicia una vez terminada la fase de Planificación, donde la entidad implementa los controles, con el fin de dar cumplimiento con los requisitos del MSPI. en la SNS se encuentra en un 6% cuando el avance esperado es de 20%.

Evaluación de desempeño: en esta fase la entidad evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 *"Protección de datos personales"*, Ley 1712 de 2014 *"Ley de Transparencia y Acceso a la Información Pública"*, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue. en la SNS se encuentra en un 6% cuando el avance esperado es de 20%.

Mejora continua: Una vez culminadas las actividades del MSPI de la fase evaluación y desempeño, se deben consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas, en la SNS se encuentra en un 6% cuando el avance esperado es de 20%.

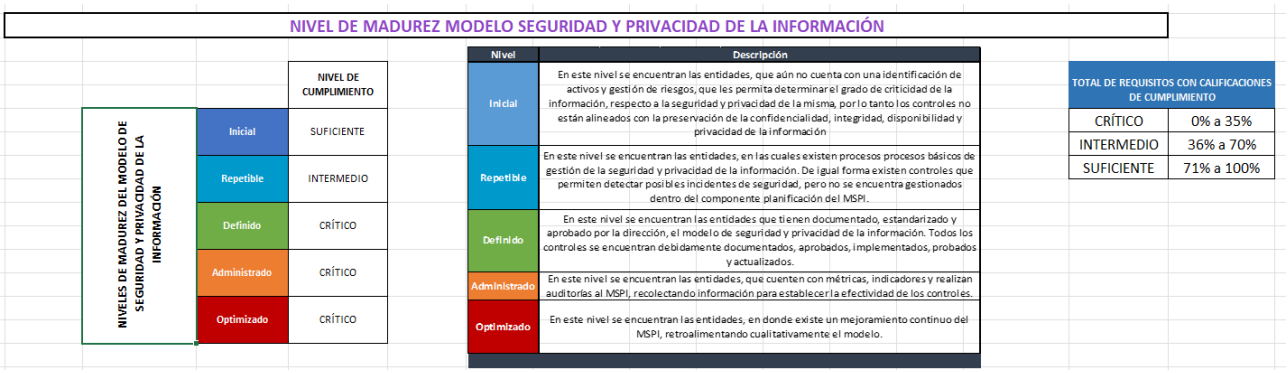


Imagen 3 Fuente la Subdirección tecnología de la Información

Con fundamento en lo anteriormente expuesto, la Oficina de Control Interno genera la **Observación N°. 10. Debilidad en el cumplimiento de anexo 1 de la resolución 00500 de 2021** al proceso de "*Gobierno y Gestión de Datos e Información*" en la actividad "*Gestionar Seguridad y Privacidad de los Datos e Información*", liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así:

Resulta importante que, desde el proceso objeto de auditoría, se adelanten los análisis de causas que motivan el bajo nivel del indicador aceptado para el cumplimiento de valoración de controles establecidos en el MSPI, a fin de determinar si estas son ajenas a la operación, o si en efecto, se encuentran asociadas a una serie aspectos inmersos dentro de las actividades que influyen en el incumplimiento como lo es la falta de recurso humano especializado en Seguridad y Privacidad de la Información (certificado en ISO 27001 de 2013), aspectos técnico – económicos, situación que fuera evidenciada por la información aportada por la DID/STI, y sustentada bajo el análisis estadístico obtenido de la información registrada en el instrumento de evaluación del MSPI y la verificación del cumplimiento del Anexo 1 resolución 00500 de 2021 de MINTIC, para que con ello

coadyuve con la toma de decisiones que resulten más favorables para garantizar la Disponibilidad, Integridad y Confidencialidad de la Seguridad y Privacidad de la Información de la SNS.

1.5 Sistema de Información (SIAD)

Como parte de las actividades que se derivan del ejercicio auditor al *"Proceso Gobierno y Gestión de Datos e Información"* en las actividades claves de éxito: *"Gestionar Seguridad y Privacidad de los Datos e Información"* y *"Gestionar aplicaciones"* que se viene adelantando por parte de la Dirección de Innovación y Desarrollo y la Subdirección de Tecnologías de la Información de la Superintendencia Nacional de Salud, dentro de la muestra alcance de la presente auditoria se solicitó información mediante radicado 20231400000118293 de 9 de agosto de 2024 enviado a la Dirección de Innovación y Desarrollo con copia a la Subdirección de Tecnología de Información. Así las cosas, en el alcance de la solicitud se pidió todo lo relacionado con los incidentes de seguridad de la información del año 2023 y los sistemas de información activos de la SNS, registrándose por parte de la DID/STI que uno de los sistemas más afectados fue el SUPERSIAD.

Así las cosas, el alcance de la presente auditoria al sistema de información de investigaciones administrativas solo se realizó la verificación y evaluaciones a las acciones adelantadas por la Superintendencia Delegada Para Investigaciones Administrativas de la SNS del incidente de seguridad de 17 de febrero y 12 de septiembre de 2023, lo que concierne al control de expedientes administrativos sancionatorios fue realizada por la Oficina de Control Interno en la vigencia 2023.

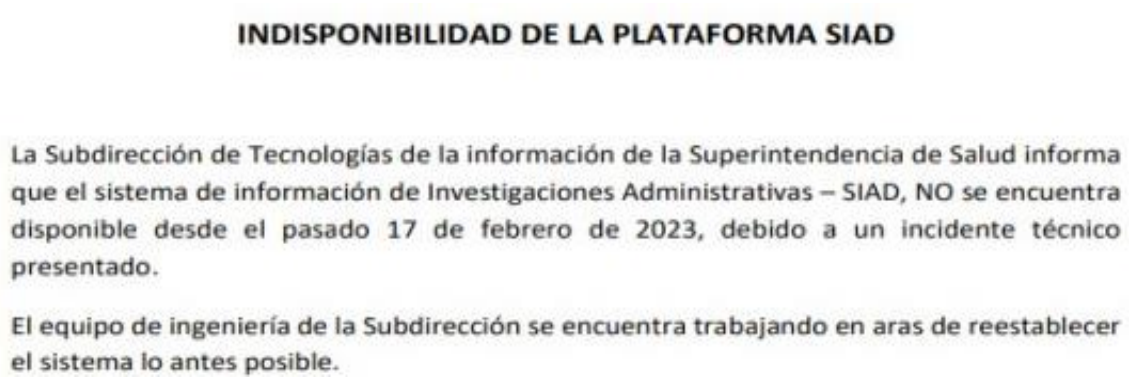
El Auditor realizó solicitud de información sobre los incidentes de seguridad y privacidad de la información a la Superintendencia Delegada Para Investigaciones Administrativas a través de correo electrónico el 14 de noviembre de 2024, de acuerdo con la información y soportes aportados por DIA y DID/STI, se evidenció lo siguiente:

De la información aportada por DIA - DID/STI

De acuerdo informe emitido por DID/STI, El sistema de información más afectado fue SUPERSIAD, correspondiente a la encriptación o secuestro de los datos registrado en las bases de datos que contienen todos los expedientes de investigaciones administrativas desde el año 2016 hasta el año 2019.

Mediante los Memorandos N° 20237000000021253 de fecha 6 de marzo de 2023, N° 20237000000022573 de fecha 9 de marzo de 2023, N° 20237000000023993 de fecha 13 de marzo de 2023 y N°20237000000029533 de fecha 28 de marzo de 2023, le reitera a la DID/STI la necesidad y la urgencia de una certificación de no funcionamiento del SIAD en la medida en que la Delegatura para Investigaciones Administrativas no tenía acceso a una fuente oficial de la Supersalud para generar respuestas y reportes al señor Superintendente Nacional de Salud, delegadas de la Supersalud, entes de control, derechos de petición y demás solicitudes internas y externas. Al respecto no hubo respuesta por parte de dicha Dirección.

La DID/STI da respuesta a la DIA a través del Memorando N° 20231530000030223 de fecha 29 de marzo de 2023, en el cual el entonces subdirector de tecnologías de la información generó un certificado de disponibilidad, tal como se evidencia en la siguiente imagen:



INDISPONIBILIDAD DE LA PLATAFORMA SIAD

La Subdirección de Tecnologías de la información de la Superintendencia de Salud informa que el sistema de información de Investigaciones Administrativas – SIAD, NO se encuentra disponible desde el pasado 17 de febrero de 2023, debido a un incidente técnico presentado.

El equipo de ingeniería de la Subdirección se encuentra trabajando en aras de reestablecer el sistema lo antes posible.

Mediante Memorando N° 20237000000026823 de fecha 21 de marzo de 2023 la Delegatura para Investigaciones Administrativas le solicitó a la DID dentro del proyecto de fábrica de software, un tablero de control de SharePoint, un buscador SharePoint y una nueva herramienta de investigaciones administrativas. Mediante Memorando N° 20237000000049503 del 17 de mayo de 2023 se solicitó a la dependencia tomar acciones pertinentes para el mantenimiento y reparación del SIAD; mediante Memorando N° 20237000000059683 de fecha 13 de junio de 2023 se expide una nueva certificación de indisponibilidad del SIAD, y se establecieron acciones para que se pueda acceder a la información del SIAD desde el año 2007 al año 2016 y una nueva herramienta tecnológica en reemplazo del SIAD, aduciendo que a la fecha no se contaba con una fuente de información institucional de expedientes administrativos sancionatorios desde el año 2016 a la fecha.

A través del Memorando N° 20231530000083823 de fecha 11 de agosto de 2023 la Dirección de Innovación y Desarrollo dio respuesta a los documentos identificados con radicados N°20237000000026823 de fecha 21 de marzo de 2023 y N° 20237000000059683 de fecha 13 de junio de 2023, poniendo de presente lo siguiente:

- Que no era procedente generar un certificado de indisponibilidad, en la medida en que el SIAD estaba disponible para la consulta de expedientes administrativos desde el 03 de febrero de 2002 hasta el año 2016.
- Señaló además que el acceso al SIAD estaba disponible tanto en internet Explorer (https://siad.supersalud.gov.co/SIAD/Login.aspx), como en los demás navegadores (http://supersiad/SIAD/Login.aspx.).
- Respecto a la información institucional de los expedientes administrativos del año 2016 en adelante y que a la fecha no se evidencia registro alguno, la Subdirección de Tecnologías manifestó que estaba avanzando en los procedimientos de contratación de herramientas que permitiesen desarrollar las necesidades institucionales.

Análisis de la Oficina de Control Interno

Conforme la información aportada, soportes y la prueba de recorrido realizada el 25 de noviembre y Teniendo en cuenta los antecedentes que se acaban de relacionar y con el fin de dar cumplimiento

al objetivo de la presente auditoría, vale decir, *"(…) dar a conocer a la Alta Dirección la adecuada operación de los Sistemas de Información de la Superintendencia Nacional de Salud (…)"*, a continuación se registran los resultados de la evaluación realizada a SIAD, la cual se llevó a cabo durante los meses de agosto a diciembre de 2024 evidencio lo siguiente:

- Se evidenció falta de respuesta oportuna por parte de DID/STI a los requerimientos realizados por parte de la DIA.
- No se evidenció documentado de manera técnica y detallada la afectación que genero el incidente de seguridad y privacidad de la información al sistema de información SUPERSIAD.
- Por parte de la DIA se estableció un plan de recuperación de la data de las investigaciones administrativas del año 2066 al 2019, no obstante, por parte del auditor no se evidenció el porcentaje de recuperación de la data y tampoco que este documentado todas las acciones en una base de conocimientos de investigaciones administrativas con todas sus actuaciones dentro de los expedientes.
- El registro de expedientes con sus respectivas actuaciones se está realizando en un archivo Excel donde las condiciones de accesos, roles y seguridad es mínimo.
- El auditor de la OCI observó que desde el año 2021, 2022 y 2023 dentro de los informes de auditoria la Oficina de Control Interno, se ha venido realizando recomendaciones y observaciones con el fin de que desde DID y la STI se implemente un sistema de información automatizado, seguro y robusto para las investigaciones administrativas de la SNS y hasta la fecha no se ha dado solución a esta situación.

Las situaciones anteriores han generado la no disponibilidad, integridad y disponibilidad de la información de las investigaciones administrativas, además de no disponer de un plan de contingencia establecido y por ello los tiempos de recuperación de la data ha sido compleja, también se evidenció que no hay una base de conocimientos de las investigaciones administrativas.

Con fundamento en lo anteriormente expuesto, el Auditor de la Oficina de Control Interno genera la **No conformidad N°. 4. Incumplimiento en la implementación del sistema de información de investigaciones administrativas** al proceso *"Gobierno y Gestión de Datos e Información"* en la actividad clave de éxito "*Gestionar solicitudes de la Dirección de Innovación y Desarrollo"* y *"Gestionar Aplicaciones"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así:

La Oficina de Control Interno eleva no conformidad al proceso *"Gobierno y Gestión de Datos de Información"* - actividad clave de éxito *"Gestionar problemas y cambios"* liderado por la Dirección de innovación Desarrollo, ante el incumplimiento **en la implementación del sistema de información de investigaciones administrativas,** falta de respuesta oportuna por parte de DID/STI a los requerimientos realizados por parte de la DIA, no se evidenció documentado de manera técnica y detallada la afectación que genero el incidente de seguridad y privacidad de la información al sistema de información SUPERSIAD, aspecto que resulta importante intervenir que permitirán manejar adecuadamente situaciones como las presentadas en 2023, logrando mitigar de manera acertada la materialización de riesgos, y con los cuales se podría generar una base de conocimientos para garantizar la integridad, confidencialidad, y la disponibilidad de los sistemas de información y de infraestructuras, así mismo se contemple un plan de actualizaciones y mantenimientos al nuevo sistema de información que permita garantizar su usabilidad, funcionalidad y disponibilidad en el tiempo y se ajuste a la normatividad vigente que aplique a las investigaciones administrativas y a las dependencias que hagan parte de esa solución que garanticen la disponibilidad, integridad y confidencialidad de la información que se administra, se recolecta y se trata en la Superintendencia delegada de Investigaciones Administrativas.

1.6. Plan de Continuidad del Negocio – incidentes de seguridad.

La Oficina de Control Interno de la Superintendencia Nacional de Salud, en cumplimiento de las funciones asignadas por la Ley, en especial, lo preceptuado en la Ley 87 de 1993 y demás normas concordantes y en atención a las actividades definidas en el Plan Anual de Gestión – PAG correspondientes a la vigencia 2023 y de 1 de enero a julio 31 de 2024, dentro del alcance de presente auditoria su ejecución del mes de agosto a diciembre de 2024, realizó seguimiento a la gestión adelantada por la Superintendencia Nacional de Salud para garantizar la continuidad del negocio, relacionados con los temas objeto de verificación, de acuerdo al alcance definido.

Para efectos de validar las acciones adelantadas por la Entidad para dar cumplimiento a lo establecido en la guía de MINTIC, la Oficina de Control Interno requirió información a Secretaría General, a la Subdirección de Tecnologías de la Información y a la Superintendencia Delegada de Investigaciones Administrativas, formulando preguntas relacionadas con los lineamientos de la mencionada guía, que permitieran al Auditor analizar las gestiones de esas dependencias para garantizar la continuidad de sus operaciones, de lo cual se registrará de manera general el resultado de lo analizado.

La actualización del plan de continuidad del negocio más reciente es del año 2021, donde la Superintendencia Nacional de Salud incluye dentro de este plan información documentada que guía a la SNS para responder a una interrupción y reanudar, recuperar y restaurar la entrega de productos y servicios de acuerdo con sus objetivos de continuidad del negocio

Esto con fin de contar con una herramienta que le permita a la SNS prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo al personal que presta sus servicios para la Entidad y los visitantes de la sede principal, que afecten el debido desarrollo de las actividades propias de SNS, impedir la prestación y continuidad del servicio a los Grupos de Valor o el cumplimiento de los compromisos establecidos en la planeación estratégica institucional, la Entidad ha consolidado el conjunto de acciones que se emprenden para dar respuesta a estos eventos en el Plan de continuidad del negocio.

Se establecen los lineamientos en el Decreto 1078 de 2015. por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones para que las entidades de orden nacional y territorial garanticen la disponibilidad y la recuperación de la operación del negocio en caso de que se presente un evento adverso así:

> *"TÍTULO 17. Lineamientos generales en el uso y operación de los servicios ciudadanos digitales"*.
>
> *"ARTICULO 2.2.17.1.6. Principios. Además de los principios previstos en el artículo 209 de la Constitución Política, en el artículo 2 de la Ley 1341 de 2009, en el artículo 3 de la Ley 1437 de 2011, en el artículo 4 de la Ley 1581 de 2012 y los atinentes a la Política de Gobierno Digital contenidos en el artículo 2.2.9.1.1.3 del capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015 la prestación de los servicios ciudadanos digitales se orientará por los siguientes principios:*
>
> *6. Seguridad, privacidad y circulación restringida de la información: Toda la información de los usuarios que se genere almacene, transmita o trate en el marco de los servicios ciudadanos digitales deberá ser protegida y custodiada bajo los más estrictos esquemas de seguridad digital y privacidad con miras a garantizar la autenticidad, integridad, disponibilidad. confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en el habilitador transversal de seguridad de la información de la Política de Gobierno Digital. (negrilla fuera de texto)*
>
> *ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y* ***continuidad*** *de la prestación del servicio. en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital. que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo."*

Conforme a lo expuesto con relación al contexto y al marco legal que debe contemplar el plan de continuidad del negocio de la SNS, el Auditor de la Oficina de Control Interno realizó solicitud de información con memorando 20241400000080393 de 9 de agosto de 2024 y con correo electrónico del 21 de octubre de 2024, donde se adjuntaron las matrices *"**plan continuidad_STI_2024.xlsx**"* y Matriz del Plan de contingencia – incidentes de seguridad de la información *"**Plan de Contingencia_2023_2024.xlsx**"*. con su respectivo cuestionario para que lo diligenciara la DID/STI y la Secretaria General, con base en la información y los soportes aportados por estas dependencias, el auditor de la OCI evidenció lo siguiente:

- No se evidenció actualización del Plan de Continuidad del Negocio de la SNS, la última actualización fue del 2021
- La Entidad no cuenta con procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales.
- No se encuentra documentada la actuación frente a las contingencias y no se ha actualizado el plan de contingencia; tampoco se observó algún trámite que se haya adelantado en ese sentido
- No se han adelantado las acciones para ajustar y/o mejorar el BIA de la Entidad.
- No se tiene definido el plan de contingencias de la Entidad y no han sido socializado a la Entidad tanto a los líderes de procesos como a sus equipos de trabajo
- No se aportó por parte de DID/STI y la secretaria general, soportes sobre simulacros realizados, resultados y lecciones aprendidas.

Frente a la gestión de incidentes se realizó seguimiento y evaluación en capitulo gestión de incidentes.

Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **No conformidad N°. 5. Incumplimiento al ARTICULO 2.2.17.1.6. y al ARTÍCULO 2.2.17.5.6 del decreto 1078 de 2015** al proceso *"Gobierno y Gestión de Datos e Información"* en la actividad *"Gestionar TI"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información así:

La Oficina de Control Interno eleva no conformidad al proceso *"Gobierno y Gestion de Datos de Información"* - actividad clave de éxito *"Gestionar problemas y cambios"* liderado por la Dirección de innovación La Oficina de Control Interno eleva no conformidad al proceso *"Gobierno y Gestion de Datos de Información"* - actividad clave de éxito "Gestionar TI" liderado por la Dirección de innovación Desarrollo y al proceso *"Direccionamiento estratégico"* liderado por Oficina Asesora de Planeación, ante el incumplimiento en lo preceptuado en el **ARTICULO 2.2.17.1.6. y al ARTÍCULO 2.2.17.5.6 del decreto 1078 de 2015**, al no estar actualizado el Plan de Continuidad del Negocio de la SNS, no se cuenta con procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales, no está documentada la actuación frente a las contingencias, no se ha realizado el Impacto del Negocio BIA. La Oficina de Control interno insta a que se realice la actualización del plan de continuidad del negocio con su correspondiente BIA y el plan de contingencia que corresponda a la estructura organizacional, Así mismo documentar de manera estructurada todos los procedimientos, guías, tramites y socialización o capacitaciones y documentar todas las acciones adelantadas por la entidad con respecto a simulacros, incidentes y planes de contingencia, y así lograr mitigar de manera acertada la materialización de riesgos, garantizar los recurso tanto humanos, técnicos, económicos y con los cuales se podría generar una base de conocimientos para garantizar la integridad, confidencialidad y la disponibilidad de los sistemas de información y de infraestructuras físicas y tecnológicas de la SNS.

1.7 Gestión de Incidentes de Seguridad de la información

Conforme la información suministrada por DID/STI frente a la gestión de incidentes de seguridad de la información del 17 de febrero y 12 de septiembre de 2023 y los hallazgos, recomendaciones plasmadas en el informe de Auditoría a sistemas de información de la Superintendencia Nacional de Salud. 1. Procesos *"Provisión de soluciones tecnológicas"*, *"Gestión Servicios Tecnológicos"* y *"Gobierno y Gestión de la Información"*, ahora proceso *"Gobierno y Gestión de Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo. 2. Procesos Precontractual, Contractual y Post-Contractual, ahora proceso *"Gestión de Bienes y Servicios"*, liderado por la Dirección de Contratación, el auditor de la Oficina de Control Interno revisó los hallazgos plasmados en el informe de auditoría 2023, los documentos y soportes aportados por DID/STI, evidenciando que se siguen presentando las mismas desviaciones, y no se evidenciaron planes de mejoramiento los incidentes de la referencia 2023:

> *"De los contratos en ejecución, el equipo auditor de la OCI revisó cuáles contratos tienen relación directa con el incidente de seguridad de la información, encontrado el contrato 158 de 2022, OC 100934 de 2022, celebrado en los siguientes términos:*
>
> *A. INFORMACIÓN DEL CONTRATO*
> *- Contratista: IFX NETWORKS COLOMBIA S.A.S. - Identificación: 830.058.677-7*
> *- Fecha de suscripción del Contrato: 30/11/22*
> *- Objeto: Prestar Servicios de Nube Privada para la SNS, bajo el Acuerdo Marco que se encuentre vigente.*
> *- Plazo de Ejecución: 11 meses*
> *- Fecha de Iniciación: 16/12/2022 - Fecha de Finalización: 15/11/2023*
> *- Obligaciones del proveedor: están establecidas en la cláusula No. 11 del Acuerdo Marco para la prestación de Servicios de Nube Privada AMP CCE-916-1- AMP-2019 celebrado entre Colombia Compra Eficiente y IFX Networks Colombia S.A.S*
>
> *Obligaciones contrato 158 de 2022 - OC 100934 de 2022 relacionados con el ciberataque del 17-02-2023*
>
> *OBLIGACIÓN No. 11.38: Garantizar la protección de datos e información entregada por las Entidades Compradoras. El Supervisor informa que: El contratista cuenta con un plan de seguridad de la información, el cual se incorporó al repositorio de la carpeta contractual https://supersalud.sharepoint.com/OTI/GestAdq/ V_2022/IFX_Networks/SitePages/Home.aspx enero de 2023.*
>
> *Según lo indicado por el Supervisor del contrato por parte de la SNS; "(…) esta obligación aplica directamente con Colombia Compra Eficiente, quien adelanta lo pertinente con el contratista, de acuerdo con lo establecido en el numeral 13.7 "Hacer seguimiento al cumplimiento de las obligaciones derivadas del presente acuerdo marco a cargo de los proveedores y de las entidades compradoras" de la cláusula 13 Obligaciones de Colombia Compra Eficiente", lo que indica que ¿la SNS no realiza controles frente a la protección de los datos e información entregada a IFX?*

OBLIGACIÓN No. 11.39: Buscar la causa raíz de las Fallas que afectan la prestación de los Servicios de Nube Privada y proporcionar solución a ellas en el tiempo establecido en los ANS

En el informe de supervisión del mes de febrero de 2023, el supervisor argumenta que para dicho periodo, se reportaron incidencias que no afectaron la prestación del servicio y autoriza el pago al contratista, desconociendo abiertamente que nueve (9) sistemas de información de la SNS presentaron indisponibilidad para los usuarios y finalmente uno (1) de ellos, presentó pérdida de información, que corresponde al SIAD en el periodo comprendido entre el año 2016 y febrero del 2023.

OBLIGACIÓN NO. 11.40: Contar con sistemas de respaldo definidos en las condiciones transversales que permitan la prestación de los Servicios de Nube Privada cuando haya una Interrupción.
Esta obligación aplica directamente con Colombia Compra Eficiente, quien adelanta lo pertinente con el contratista, de acuerdo con lo establecido en el numeral 13.7 "Hacer seguimiento al cumplimiento de las obligaciones derivadas del presente acuerdo marco a cargo de los proveedores y de las entidades comprados" de la cláusula 13 Obligaciones de Colombia Compra Eficiente.

El supervisor desconoce que respecto del sistema SIAD en el ataque cibernético del 17/02/2023 se perdió la información del período comprendido entre el año 2016 y febrero del 2023, porque en el mismo NODO se tenían configuradas las aplicaciones y las copias de seguridad de la información y al ocurrir la afectación de las aplicaciones, se perdió la información y a la fecha de presentación de este informe, no ha sido restaurada.
Obligación No. 11.44: Establecer y ejecutar planes de contingencia cuando ocurran eventos de fuerza mayor o caso fortuito que afecten la prestación de los Servicios de Nube Privada.

Sin embargo, esta obligación aplica directamente con Colombia Compra Eficiente, quien adelanta lo pertinente con el contratista, de acuerdo con lo establecido en el numeral 13.7 "Hacer seguimiento al cumplimiento de las obligaciones derivadas del presente acuerdo marco a cargo de los proveedores y de las entidades comprados" de la cláusula 13 Obligaciones de Colombia Compra Eficiente.

En los soportes de los pagos y en los informes no se dejó constancia de algún plan de contingencia elaborado y aplicado al incidente de seguridad de la información ocurrido el 17/02/2023."

Análisis del Auditor

"De acuerdo con la verificación contractual realizada, se coligen debilidades en la supervisión del contrato en mención, toda vez que el Supervisor certificó el cumplimiento de las obligaciones del contratista, a pesar del incidente de seguridad de la información por ataque cibernético que afectó la disponibilidad de los servicios, el respaldo de las operaciones realizadas y no se tomaron las medidas inmediatas para la recuperación de la información, y más grave aún, no se iniciaron estudios, análisis e investigaciones para determinar el posible incumplimiento en las obligaciones plasmadas en el Acuerdo marco de precios 158 de 2022 y específicamente en la Orden de Compra 100934 de 2022; así mismo no se dejaron registros de lo ocurrido el 17/02/2023 en los informes de supervisión, así como la falta de publicidad de los pagos e informes de supervisión en "Colombia Compra Eficiente".

Por lo expuesto, el equipo auditor de la OCI genera la Observación N. 2.2.11 del presente informe"

La Oficina de Control Interno, una vez realizada la verificación y trazabilidad a las acciones adelantadas y la información aportada por la DID/STI frente a los hallazgos plasmados en el informe de auditoría 2023, concluye que se siguen presentando los siguientes aspectos:

Para los dos (2) incidentes de seguridad presentados en la vigencia 2023, se observa que la entidad no cuenta con un modelo estructurado de gestión para la *"atención de incidentes de seguridad de la información"*, ni un plan de contingencia,

Aunado a esto la DID/STI no tiene definido un procedimiento, ni una matriz o bitácora en la que se relacionen incidentes de seguridad.

Ante el ciberataque presentado que afectó los principios de la Seguridad de la Información de la SNS, Disponibilidad, Integridad y Confidencialidad de la información y habiendo realizado un diagnóstico y análisis del estado de protección y maduración de la Política de Seguridad Digital y Gobierno Digital en la Entidad, la DID/STI no han iniciados las acciones para prevenir, contener y mitigar este tipo de incidentes de seguridad y privacidad de la información

La Oficina de Control Interno conforme la información aportada por la DID/STI evidenció que se hicieron análisis de vulnerabilidades en febrero 2023 y agosto de 2024 a algunos sistemas de información y no se observó que se haya subsanado y haya habido remediación de los análisis realizados.

El Auditor también evidenció las siguientes situaciones:

• Deficiente gestión de riesgos (análisis y controles de mitigación)
• Se evidenció que persiste la falta de adopción de buenas prácticas de administración, monitoreo y gestión para la infraestructura TI.
• No se evidenció matriz de roles y responsabilidades de gestión de incidentes de seguridad.
• Existe un desconocimiento de la Infraestructura tecnológica que soporta los sistemas de información críticos y las infraestructuras críticas de la SNS
• No se evidenciaron monitoreos periódicos con sus correspondientes soportes, que permitan definir una línea base para cuando se presente un incidente
• No se encuentran implementadas y aprobadas las políticas de: *"Gobierno y Seguridad Digital"*.
• No se evidenció actualización de riesgos de seguridad y privacidad de la información 2024.
• No se ha establecido la documentación necesaria que dé soporte en la gestión de incidentes de seguridad de la información.
• No se evidenció procedimiento y/o guías actualizados de manejo de incidentes de seguridad de la información
• No se evidenciaron soportes y acciones realizadas de monitoreos periódicos, que permitan definir una línea base para cuando se presente un incidente.
• No se evidenció una base de conocimiento para posteriores eventos o incluso para cuando se presenta alta rotación de personal (como se evidenció en la trazabilidad de este informe) exigiendo la correspondiente transferencia de conocimiento y entrega de cargos de manera formal y oficial.

• No se evidenció seguimiento y verificación de resultados de las investigaciones adelantadas con respecto al incidente (denuncias internas y externas).
• No se evidenció gestión de eventos de seguridad de la información.
• No se evidenció configuración de las alertas que sean necesarias para detectar a tiempo la ocurrencia de un incidente, garantizando la aplicabilidad al interior de la entidad y la exigencia de su cumplimiento, a los proveedores.

Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno se **reitera la No conformidad N°. 1. Incumplimiento de Articulo 9 Gestión de incidentes de la resolución 00500 de 2021** al proceso de *"Gobierno y Gestión de Datos e Información"* de la actividad "*Gestionar Seguridad y Privacidad de los Datos e Información*" *y "Gestionar Problemas y Cambios*", liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnologías de la Información así:

La Oficina de Control Interno eleva no conformidad al proceso "*Gobierno y Gestion de Datos de Información*" - actividad clave de éxito "*Gestionar problemas y cambios*" liderado por la Dirección de innovación Desarrollo y al proceso "Direccionamiento estratégico" liderado por Oficina Asesora de Planeación, ante el incumplimiento preceptuado en el **Articulo 9 Gestión de incidentes de la resolución 00500 de 2021** al no gestionarse incidentes de seguridad y privacidad de la información con oportunidad, y calidad frente a la transferencia de conocimiento, Base de conocimiento (lecciones aprendidas), una adecuada gestión de riesgos, seguimiento y monitoreo a la gestión de incidentes y actualización de procedimientos definidos para atender dichos incidentes aspecto que resulta importante intervenir que permitirán manejar adecuadamente situaciones como las presentadas en 2023, logrando mitigar de manera acertada la materialización de riesgos, y con los cuales se podría generar una base de conocimientos para garantizar la integridad, confidencialidad, y la disponibilidad de los sistemas de información y de infraestructuras.

Es importante que se defina un modelo de gestión de incidentes de seguridad de la información conforme lo establece el Artículo 9 de la Resolución 00500 de 2021: *"ARTÍCULO 9. Gestión de incidentes de seguridad digital. Los sujetos obligados deben establecer un procedimiento de gestión de incidentes de seguridad digital, para realizar el tratamiento, investigación y gestión de los incidentes de seguridad digital que se presente en relación con los activos de información de cada proceso, para lo cual deben: 1. Gestionar los incidentes de seguridad digital, según el procedimiento establecido por MinTIC, para lo cual deben crear una bitácora que contenga la descripción de cada una de las actividades desarrolladas en la gestión de estos; 2. Designar dentro de la entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital; 3. Una vez identificado el incidente de seguridad digital se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave y Grave por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación del CSIRT Gobierno; 4. Los incidentes catalogados por el responsable de seguridad digital de la entidad, como Menos Grave y Menor, deben ser comunicados al CSIRT Gobierno en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos; 5. Los sujetos obligados, según el análisis e investigación de los incidentes y teniendo en cuenta la causa raíz, deben realizar los respectivos planes de mejoramiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento."*, además, que incluya aspectos como los activos de información

críticos e infraestructuras críticas con enfoque en la *"ciberseguridad"*, lo cual redundará en el establecimiento de estrategias que permitan implementar medidas técnicas, operativas, legales, organizacionales, determinando el paso a paso de cada acción, estableciendo roles y responsabilidades. Es importante, además, que se comience de manera prioritaria esta gestión, con ocasión de los incidentes de seguridad presentados en 2023, lo cual debe quedar documentado y soportado, incorporando las lecciones aprendidas y actividades desarrolladas para la atención de estos eventos;

1.8 Matriz de Roles y Responsabilidades de la Superintendencia Nacional de Salud - Formato "DEFT12" – V1.

Partiendo de la premisa que, la Matriz de Roles y Responsabilidades incorpora la definición de los nuevos roles de manera articulada con las áreas, y que se lleva a cabo a través de mesa de trabajo, esto con el objeto de, determinar los responsables de las actividades que se deben ejecutar en el marco de las funciones y competencias que reza el Decreto 1080 de 2021, desde la Oficina Asesora de Planeación de la Entidad, en su Actividad Clave de Éxito *"Liderar y Articular el Sistema Integrado de Gestión"*, específicamente en la fase *"Actualizar Roles y Responsabilidades"*, tiene definido el formato *"DEFT12 – Matriz de Roles y Responsabilidades"*, al respecto, no se observó por parte del Auditor de la Oficina de Control Interno que, el proceso *"Gobierno y Gestión de Datos e Información"* para el periodo evaluado, esto es, vigencia 2023 y primer semestre de 2024, tuviera diligenciado el citado formato de Matriz de Roles y Responsabilidad de Seguridad y Privacidad de la Información y de la STI que permita la validación y verificación de los responsables de cada actividad, como también lo es que, no se observó que, desde la Oficina Asesora de planeación se haya adelantado actividades de seguimientos tendientes a coadyuvar a garantizar su diligenciamiento, dado que, la citada fase determina que: "*El profesional realiza la revisión de los roles y responsabilidades del SIG y revisa si se requiere ajuste o es necesario definir nuevos roles de manera articulada con las áreas, a través de mesas de trabajo. Las modificaciones o ajustes irán acordes con la elaboración y control de documentos*".

Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno **reitera la No Conformidad N°. 2. Incumplimiento de la definición de roles y responsabilidades de Seguridad y Privacidad de la información y de TI de la SNS**, a los procesos "*Gobierno y Gestión de Datos e información*", liderado por la Dirección de Innovación y desarrollo, y; "*Direccionamiento Estratégico*" actividad calve de éxito" *Liderar y articular Sistema Integrado Gestion*, liderado por la Oficina Asesora de Planeación, así:

Realizado el análisis de la información objetiva aportada por el proceso objeto de evaluación independiente, no se observó el diligenciamiento del Formato "*DEFT12 – Matriz de Roles y Responsabilidades*" por parte del proceso "*Gobierno y Gestión de Datos e Información*" a cargo de la Dirección de Innovación y desarrollo, como también lo es que, no se logró identificar el seguimiento y revisión a cargo del proceso "*Direccionamiento Estratégico*" liderado por la Oficina Asesora de Planeación, aunado a la debilidad en el principio de *"Autocontrol"* que dispone el "*Modelo Estándar de Control Interno (MECI)",* esto por parte del proceso para detectar desviaciones y con ello efectuar correctivos para la adecuada ejecución de las actividades y/o tareas bajo su responsabilidad, y que representan oportunidad de mejora para el adecuado desarrollo de las Actividad Clave de Éxito objeto de análisis y evaluación.

1.9 Mapa de Riesgos de Seguridad y Privacidad de la información

El auditor de la Oficina de Control Interno, conforme solicitud de la Matriz de Riesgos de Seguridad y Privacidad de la Información con memorando 20241400000080393del 9 de agosto de 2024 al DID/STI, a la cual se aportó el formato para el diligenciamiento del Mapa de Riesgos de Seguridad y Privacidad de la Información – DEFT24 V1 del 22/09/2023, el Auditor evidenció que esta matriz no ha sido diligenciada por la DID/STI y también observó que por parte de la Oficina Asesora de Planeación haya habido una comunicación solicitando el diligenciamiento del Mapa de Riesgos de Seguridad y Privacidad de la Información – DEFT24 de la SNS.

Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **No Conformidad N°. 6. Incumplimiento en el diligenciamiento Mapa de Riesgos de Seguridad y Privacidad de la Información – DEFT24**", a los procesos "*Gobierno y Gestión de Datos e información*", liderado por la Dirección de Innovación y desarrollo, y; "*Direccionamiento Estratégico*" actividad calve de éxito "*Gestionar Riesgos*", liderado por la Oficina Asesora de Planeación, así:

Realizado el análisis de la información objetiva aportada por el proceso objeto de evaluación independiente, no se observó el diligenciamiento del Formato "DEFT24" – *"Mapa de Riesgos de Seguridad y Privacidad de la Información*" por parte del proceso "*Gobierno y Gestión de Datos e Información"* a cargo de la Dirección de Innovación y desarrollo, como también lo es que, no se logró identificar el seguimiento y revisión a cargo del proceso *"Direccionamiento Estratégico"* liderado por la Oficina Asesora de Planeación, aunado a la debilidad en el principio de *"Autocontrol"* que dispone el *"Modelo Estándar de Control Interno (MECI)"*, esto por parte del proceso para detectar desviaciones y con ello efectuar correctivos para la adecuada ejecución de las actividades y/o tareas bajo su responsabilidad, y que representan oportunidad de mejora para el adecuado desarrollo de las Actividad Clave de Éxito objeto de análisis y evaluación.

1.10 Proceso de Gestión de Bienes y Servicios

Conforme a la Auditoría de gestión interna que se está ejecutando a los procesos: *"Gobierno y Gestión de Datos e Información"* actividades claves de éxito *"Gestionar TI"* y *"Gestionar Seguridad y Privacidad de los Datos e Información"*, *"Gestión de Bienes y Servicios"* en relación con los contratos suscritos para prestar los servicios de nube pública y nube privada de la SNS de las vigencias 2023 y 2024.

Se solicitó al respecto, el informe de supervisión del nuevo contrato de renovación del *"licenciamiento de productos Microsoft para fortalecer el diseño y desarrollo de servicios y soluciones de tecnologías de la información para el cumplimiento de las funciones de la Superintendencia Nacional de Salud"*, que remplazó al contrato 156 de 2023 con orden de compra 117620 – IAD Software I – Microsoft, así mismo la orden de compra, el certificado de instalación de las licencias por parte del proveedor

Con correo electrónico el día 4 de diciembre dio respuesta la Dirección de Contratación en los siguientes términos:

> *"Damos atención a su solicitud de información, según la cual requiere "se allegue el* ***informe de supervisión del nuevo contrato de renovación del "licenciamiento de productos Microsoft para fortalecer el diseño y desarrollo de servicios y soluciones de tecnologías de la información para***

el cumplimiento de las funciones de la Superintendencia Nacional de Salud*", que remplazo al contrato 156 de 2023 con orden de compra 117620 – IAD Software I – Microsoft,* ***así mismo la orden de compra****,* ***el certificado de instalación de las licencias por parte del proveedor".*** (Negrilla fuera de texto)

Sobre el particular la Dirección de Contratación le informa que previo adelantamiento de proceso de contratación a través de la modalidad de Selección Abreviada para la adquisición de bienes y servicios de características técnicas uniformes en Bolsas de Productos, la Superintendencia Nacional de Salud celebró con AGROBOLSA S.A. - Comisionista de Bolsa, el Contrato de Comisión No. 162 de 2024 cuyo objeto consiste en: "Establecer las condiciones generales que regirán el negocio de comisión frente a la operación para: "Adquirir y renovar el soporte y licenciamiento de Microsoft para el cumplimiento de las funciones de la Superintendencia Nacional de Salud", de conformidad con el procedimiento establecido en el Reglamento de Funcionamiento y Operación de la Bolsa para el Mercado de Compras Públicas MCP de la Bolsa Mercantil de Colombia."

Ahora bien, teniendo en cuenta las etapas del proceso de Selección Abreviada por Bolsa de Productos, se señala que el viernes 29 de noviembre de 2024 se llevó a cabo la rueda de negocios - operación en bolsa No. 69486369.0, en la cual se seleccionó el proveedor de las licencias, es decir, en la fecha referida fueron adjudicadas las licencias.

A la fecha, nos encontramos a la espera de las pólizas por parte del "Comitente Vendedor", que para el caso es la firma CONTROLES EMPRESARIALES, teniendo en cuenta el plazo de ejecución conforme a la ficha técnica de negociación y el Manual de Operación de la Bolsa Mercantil, es el siguiente:

El plazo para la entrega de las licencias junto con los códigos de activación por parte del comitente vendedor objeto de la presente negociación será de quince (15) días calendario , contados a partir del sexto (6) día hábil siguiente a la rueda de negociación, previa suscripción del acta de inicio la cual deberá suscribirse dentro del siguiente día hábil de la negociación, por parte del comitente vendedor, comisionista vendedor, el supervisor de la negociación designado por el comitente comprador y el comisionista comprador, previo cumplimiento de los requisitos de ejecución, es decir expedición del registro presupuestal y aprobación de las garantías única y adicionales señaladas en la presente ficha por parte del comitente comprador, una vez sea constituida y presentada ante el comitente comprador en debida forma por el comitente vendedor, así como la constitución de las garantías fijadas por el Sistema de Compensación y Liquidación de la Bolsa, en los términos de su reglamento.

La entrega de los códigos para la activación de las licencias deberá realizarse al correo electrónico del supervisor designado.

De acuerdo con la renovación del uso de las suscripciones de las licencias, éstas deberán estar activas por el plazo de doce (12) meses contados a partir de la activación de los códigos de suscripción.

De esta manera, se precisa que las licencias fueron adquiridas el pasado viernes 29 de noviembre de 2024, sin embargo, a la fecha no se tiene pólizas por lo que el contrato no ha iniciado.

Por último, se indica, que el 3 de diciembre de 2024 se preguntó por las pólizas a la firma comisionista quien informa que aún no cuenta con ellas para enviarlas a la entidad, pero que, de acuerdo con los documentos que rigen la operación en bolsa se encuentran dentro del plazo para entregarlas.

Por lo expuesto se remite copia de los siguientes documentos:

***1.** Contrato electrónico No. 162 de 2024*
***2.** Anexo cláusulas contractuales Contrato de Comisión No. 162 de 2024*
***3**. Modificación No. 1 (adición y prórroga) al Contrato de Comisión No. 162 de 2024*
***4.** Ficha técnica de negociación modelo de tecnología*

Así mismo se remite copia de documentos de la rueda de negocios en la cual se seleccionó al proveedor de las licencias:

***5.** Operación de mercado abierto – rueda No. 225*
***6.** Documento de AGROBOLSA S.A. de aceptación documentos condiciones de participación - licenciamiento software Op. No. 69486369 – Contrato de Comisión No 162-2024.*
***7.** Documento de AGROBOLSA S.A. informe de adjudicación 29-NOV-24-SISTEMA INTEGRAL DE TECNOLOGÍA Y SOFTWARE - Op.–- Contrato de Comisión No. 162 DE 2024 - Orden de Compra*."

Análisis del Auditor

El Auditor verificó la información y soportes aportados por DID/STI y la Dirección de Contratación y evidenció lo siguiente:

- Que la orden de compra 11762, contrato 156 de 2023 *"Renovar el licenciamiento de productos Microsoft para fortalecer el diseño y desarrollo de servicios y soluciones de tecnologías de la información para el cumplimiento de las funciones de la Superintendencia Nacional de Salud"*, finalizó el pasado 31 de octubre de 2024.
- Que a fecha de la presente auditoria, no se observó informe de certificación del supervisor en lo referente a: ***"el certificado de instalación de las licencias por parte del proveedor".***
- No se observó la forma de pago por servicios prestados, desde el primero de noviembre a la citada certificación, aludiendo que existe un presupuesto para la vigencia 2024 y que se deben prever los recursos necesarios para el cumplimiento de esta obligación, afectación en la planificación.

Con fundamento en lo anteriormente expuesto, el auditor de la Oficina de Control Interno genera la **Recomendación N°. 8. Debilidad en el cumplimiento al principio planificación presupuestal**", a los procesos "*Gobierno y Gestión de Datos e información*" de la actividad clave de éxito *"Gestión de TI"*, liderado por la Dirección de Innovación y desarrollo, *"Gestión y Bienes y Servicios"* liderado por la Dirección de Contratación, así:

Debilidad en la definición de la forma de pago por servicios prestados, que abarca el periodo comprendido desde el 1º de noviembre a la citada certificación, aludiendo que existe un presupuesta para vigencia y que se deben prever los recursos necesarios para el cumplimiento de esta

obligación, donde puede haber una posible afectación el principio de planificación que reza en el Decreto 111 de 1996, situación está, que podría impactar de forma negativa el cumplimiento de las obligaciones adquiridas por la Entidad, denotando a su vez un debilidad en los principios del Modelo Estándar de Control Interno (MECI), principalmente en lo que trata del Autocontrol, Autogestión y Autorregulación, instando a que se evalúe la pertinencia de tomar acciones para mitigar la posible materialización de este tipo de eventos apuntando al mejoramiento continuo del proceso.

Esta recomendación se formula en el marco del rol de prevención que tienen las Oficinas de Control Interno, no obstante que la gestión esté por fuera de las fechas de cubrimiento del alcance de la presente auditoría.

2 RESUMEN DE HALLAZGOS

De conformidad con la evidencia objetiva aportada, a continuación, se relacionan los hallazgos detectados en desarrollo de la auditoría:

N°	CONFORMIDADES	PROCESO
1	Excelente disposición y participación por parte de la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la información en el desarrollo	Gobierno y Gestión de Datos e Información

N°	OBSERVACIONES	PROCESO
1	Debilidad en la formalización de entrega de cargos de exfuncionarios de la Dirección de Innovación y Desarrollo y la Subdirección de Tecnologías de la Información.	Gobierno y Gestión de Datos e Información
2	Debilidad en el cumplimiento en la aplicación de controles relacionados con políticas de seguridad y privacidad de la información	Gobierno y Gestión de Datos e Información
3	Debilidad en el cumplimiento por parte de PMU de las recomendaciones	Gobierno y Gestión de Datos e Información
4	Debilidad en el cumplimiento de la realización de Análisis de Vulnerabilidades, monitoreo, remediación y seguimiento de estas	Gobierno y Gestión de Datos e Información
5	Debilidad en la definición de Roles y Responsabilidad por falta de segregación de funciones en los Sistemas de Información Génesis y Gaudi	Gobierno y Gestión de Datos e Información, Direccionamiento Estratégico
6	Debilidad en cumplimiento de anexo 3 de la resolución 1519 de 2020	Gobierno y Gestión de Datos e Información
7	Debilidad en el cumplimiento del numeral 3.2.6 anexo 3 de la resolución 1519	Gobierno y Gestión de Datos e Información
8	Debilidad en el cumplimiento del numeral 3.2.20 anexo 3 de la resolución 1519 de 2020	Gobierno y Gestión de Datos e Información
9	Debilidad en el cumplimiento del numeral 3.2.22 del anexo 3 de la resolución 1519 de 2020	Gobierno y Gestión de Datos e Información
10	Debilidad en el cumplimiento de anexo 1 de la resolución 00500 de 2021	Gobierno y Gestión de Datos e Información
11	Debilidad en el cumplimiento al ARTICULO 2.2.17.1.6. y al ARTÍCULO 2.2.17.5.6 del decreto 1078 de 2015.	Gobierno y Gestión de Datos e Información – Direccionamiento Estratégico

N°	NO CONFORMIDADES	PROCESO
1	Incumplimiento de Articulo 9 Gestión de incidentes de la resolución 00500 de 2021	Gobierno y Gestión de Datos e Información
2	Incumplimiento de la definición de roles y responsabilidades de Seguridad y Privacidad de la información y de TI de la SNS	Gobierno y Gestión de Datos e Información
3	Incumplimiento de lo que establece la Ley 1581 de 2012 Ley de Protección de Datos	Gobierno y Gestión de Datos e Información
4	Incumplimiento en la implementación del sistema de información de investigaciones administrativas	Gobierno y Gestión de Datos e Información
5	Incumplimiento en el diligenciamiento Mapa de Riesgos de Seguridad y Privacidad de la Información – DEFT24	Gobierno y Gestión de Datos e Información

3 RESUMEN DE RECOMENDACIONES

De conformidad con la evidencia objetiva aportada, a continuación, se relacionan las recomendaciones detectadas en desarrollo de la auditoría:

N°	RECOMENDACIONES	PROCESO
1	Debilidad en el registro de actualizaciones de antivirus, firewall y sistemas operativos de los servidores de las aplicaciones de la entidad	Gobierno y Gestión de Datos e Información
2	Debilidad en la aplicación del Manual para las copias de seguridad de la Información – DIMN14	Gobierno y Gestión de Datos e Información
3	Debilidad en la aprobación de las Políticas de Seguridad y privacidad de la Información	Gobierno y Gestión de Datos e Información
4	Debilidad en el Cumplimiento del Artículo 1 de la Ley 2345 de 2023	Gobierno y Gestión de Datos e Información
5	Debilidad en la generación de reportes del Sistema de información SIVICAL	Gobierno y Gestión de Datos e Información
6	Debilidad en el cumplimiento del numeral 3.2.1 del anexo 3 de la resolución 1519 de 2020.	Gobierno y Gestión de Datos e Información
7	Debilidad en el cumplimiento del numeral 3.2.4 anexo 3 de la resolución 1519 de 2020	Gobierno y Gestión de Datos e Información
8	Debilidad en el cumplimiento al principio planificación presupuestal	Gobierno y Gestión de Datos e Información – Gestion de Bienes y Servicios

4 RESPUESTA A RESULTADOS DE AUDITORÍA (HALLAZGOS, RECOMENDACIONES) DESDE EL PROCESO AUDITADO Y ANÁLISIS OFICINA DE CONTROL INTERNO

4.1 Proceso *"Gobierno y Gestion de Datos e Información"* a cargo de la Dirección de Innovación y Desarrollo

Que mediante radicado 20241530400130463 de 26 de diciembre de 2024 la Dirección de Tecnologías de la información y la Subdirección de Tecnología de la información dio respuesta al informe preliminar con radicado 20241400000127003 del 17 de diciembre en los siguientes términos:

La Subdirección de Tecnologías de la Información, dentro de los términos establecidos para dar respuesta al Informe Preliminar Auditoría Interna de Gestión a los procesos *"Gobierno y Gestión de Datos e Información"* y *"Gestión de Bienes y Servicios"*, para la vigencia 2023 y del 1 de enero al 31 de julio de 2024, Actividades Claves de Éxito *"Gestionar TI"* y *"Gestionar Seguridad y Privacidad de los Datos e Información"*, se permite dar respuesta a lo allí establecido, en los siguientes términos:

- **Observaciones**

Por parte del proceso auditado no hubo objeción a las observaciones plasmada en el informe preliminar con radicado 20241400000127003 del 17 de diciembre de 2024.

- **No conformidades.**

No conformidad N°. 1. Incumplimiento de Articulo 9 Gestión de incidentes de la resolución 00500 de 2021.

Respuesta del proceso auditado con radicado 20241530400130463 de 26 de diciembre de 2024:

NO CONFORMIDAD No. 1 - "2.3.1 La Entidad no cuenta con una matriz de roles y responsabilidades y de segregación de funciones."

"Grupo de Seguridad

A este respecto la Subdirección de Tecnologías de la Información, dando cumplimiento a las Planes de Mejora 1426 y 1475, inicio durante la vigencia 2024, el levantamiento de la información requerida para elaborar, formalizar y socializar la Matriz de Roles, Responsabilidades y de Segregación de Funciones, cuyo plazo final para dar cumplimiento a referidos planes es el 31 de marzo de 2025. Es importante precisar que la actividad relacionada con la elaboración de la Matriz, como base para la formalización y socialización, se encuentra en un 100% de cumplimiento y ha sido remitida a la Oficina Asesora de Planeación para su aprobación, las dos actividades restantes con vencimiento para 2025, están en proceso de desarrollo. Si bien es cierto no se cuenta con la Matriz de Roles, Responsabilidades y de Segregación de Funciones, debidamente formalizada, la Subdirección de Tecnologías de la Información ha generado los planes de mejora necesarios para dar cumplimiento al tema en mención y no consideramos que se establezca una no conformidad sobre el particular."

Análisis Oficina de Control Interno: la Oficina de Control Interno evidencia que la respuesta dada por el proceso auditado no corresponde a la **No conformidad N°. 1** ***"Incumplimiento de Articulo 9 Gestión de incidentes de la resolución 00500 de 2021"*** del proceso *"Gobierno y Gestión de Datos e Información" de la actividad clave de éxito "Gestionar, Problemas y Cambios"* liderado por la Dirección de Innovación y Desarrollo, la Subdirección de Tecnología de la Información plasmada en el informe preliminar con radicado 20241400000127003 del 17 de diciembre de 2024**,** motivo por el cual se ratifica la **No conformidad N°.1**, situación que configurará seguimiento posterior por parte de la Oficina de Control Interno.

No conformidad N°. 2. Incumplimiento de la definición de roles y responsabilidades de Seguridad y Privacidad de la información y de TI de la SNS

Respuesta del proceso auditado con radicado 20241530400130463 de 26 de diciembre de 2024:

NO CONFORMIDAD No. 2 - "2.3.2 Materialización de riesgos de seguridad de la información, por vulneración de los principios de "Confidencialidad, Integridad y Disponibilidad", con los ataques cibernéticos de 2023; así mismo la materialización de riesgos de gestión definidos para la vigencia 2023."

"Actualmente la STI y el CISO han adelantado la construcción de un plan de trabajo para darle cierre a las brechas de seguridad identificadas desde el año 2023; en la vigencia 2025.

La Subdirección de Tecnologías de la Información en la actualidad por intermedio del Grupo de infraestructura y servicios TI, efectúa el seguimiento y control de las copias de seguridad a nivel de servidores físicos, virtuales y bases de datos en cuanto a los ambientes productivos. Lo anterior, por medio de la funcionalidad nativa de AZURE - Backup Vaults.

Adicional a ello, para las aplicaciones, se tienen contenedores específicos llamados Recovery Vaults los cuales funcionan como bóvedas inmutables para la prevención de ataques y la rápida restauración de la información en caso de ataques o que se vea comprometida la información.

La Superintendencia ha contratado los servicios para mitigar los riesgos cuya materialización afectaron la disponibilidad de la información. Por lo que no se acepta esta no conformidad."

Análisis Oficina de Control Interno: la Oficina de Control Interno evidencia que la respuesta dada por el proceso auditado no corresponde a la **No. conformidad N°. 2*. "Incumplimiento de la definición de roles y responsabilidades de Seguridad y Privacidad de la información y de TI de la SNS"*** al proceso *"Gobierno y Gestión de Datos e Información" de la actividad "Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información, plasmada en el informe preliminar con radicado 20241400000127003 del 17 de diciembre de 2024**,** motivo por el cual se ratifica la **No conformidad No. 2**, situación que configurará seguimiento posterior por parte de la Oficina de Control Interno.

No Conformidad N°. 3. Incumplimiento de lo que establece la Ley 1581 de 2012 Ley de Protección de Datos

Respuesta del proceso auditado con radicado 20241530400130463 de 26 de diciembre de 2024:

NO CONFORMIDAD No. 3 - "2.3.3 Incumplimiento a los lineamientos de la política del componente de seguridad de la información y seguridad digital contenida en el Manual de Políticas Institucionales, literal "c) La revisión de los riesgos de Seguridad de la Información y Seguridad Digital se llevará a cabo como mínimo una vez al año."

"Para la vigencia 2024, la Subdirección de Tecnologías de la Información, a través del Grupo de Seguridad Digital, ha realizado la reinducción a los gestores, la revisión y actualización de los riesgos de Seguridad, los cuales ya se encuentran en la herramienta de la OAP (ITS); Dadas las circunstancias la STI y el CISO han elaborado una nueva matriz para adelantar la identificación de activos y riesgos, de manera que en el próximo semestre este actualizada la entidad frente a esta actividad y cerrando diferentes brechas encontradas.

Para la vigencia 2024, la Subdirección de Tecnologías de la Información, a través del Grupo de Seguridad Digital, presento en el mes de abril ante el Comité de Gestión y desempeño Institucional los activos de información para su aprobación y publicación, una vez culminada esta etapa se dio inicio a la socialización y capacitación de los gestores de cada dependencia para hacer la revisión y actualización de los riesgos de Seguridad, de igual forma se ejecutaron los planes de mejoramientos vigentes 1452(a) " Identificación, Actualización, Aceptación de la matriz de riesgos de seguridad". con fecha de cierra 20/12/2024 y el plan 1452 (b) con la actividad "Publicación de la Matriz de Riesgos Actualizada" con fecha de cierre 20/01/2025, las evidencias de este plan de mejoramiento en ejecución se encuentran en la herramienta de la OAP (ITS), de igual forma la STI y el CISO han elaborado una nueva matriz para adelantar la identificación de activos y riesgos, de manera que en el próximo semestre este actualizada la entidad frente a esta actividad y cerrando diferentes brechas encontradas. Por tanto, no se acepta esta no conformidad."

Análisis Oficina de Control Interno: la Oficina de Control Interno evidencia que la respuesta dada por el proceso auditado no corresponde a la **No conformidad N°. 3. *"Incumplimiento de lo que establece la Ley 1581 de 2012 Ley de Protección de Datos"*** al proceso de *"Gobierno y Gestión de Datos e Información" de la actividad "Gestionar Seguridad y Privacidad de los Datos e Información"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información, plasmada en el informe preliminar con radicado 20241400000127003 del 17 de diciembre de 2024, motivo por el cual se ratifica la **No conformidad No. 3**, situación que configurará seguimiento posterior por parte de la Oficina de Control Interno.

No conformidad No 4. Incumplimiento en la implementación del sistema de información de investigaciones administrativas

Respuesta del proceso auditado con radicado 20241530400130463 de 26 de diciembre de 2024:

NO CONFORMIDAD No. 4 - "2.3.4 Incumplimiento a los lineamientos de las políticas del componente de seguridad de la información y seguridad digital para el control de accesos, en el ítem relacionado con "Gestión de contraseñas"

Las políticas de seguridad digital y protección de datos están en su última fase de aprobación, para pasar a ser presentadas al comité directivo.

Análisis Oficina de Control Interno: la Oficina de Control Interno evidencia que la respuesta dada por el proceso auditado no corresponde a la **No conformidad N°. 4***. "Incumplimiento en la implementación del sistema de información de investigaciones administrativas"* al proceso *"Gobierno y Gestión de Datos e Información"* en la actividad clave de éxito "*Gestionar solicitudes de la Dirección de Innovación y Desarrollo"* y *"Gestionar Aplicaciones"*, plasmada en el informe preliminar con radicado 20241400000127003 del 17 de diciembre de 2024**,** motivo por el cual se ratifica la **No conformidad N°. 4**, situación que configurará seguimiento posterior por parte de la Oficina de Control Interno.

No conformidad N°. 5. Incumplimiento al ARTICULO 2.2.17.1.6. y al ARTÍCULO 2.2.17.5.6 del decreto 1078 de 2015.

Respuesta del proceso auditado con radicado 20241530400130463 de 26 de diciembre de 2024:

NO CONFORMIDAD N°. 5 - "2.3.5 Incumplimiento de las políticas del componente de Seguridad de la Información y Seguridad Digital "respaldo de la información".

"Actualmente el Grupo de infraestructura y servicios TI, efectúa el seguimiento y control de las copias de seguridad a nivel de servidores físicos, virtuales y bases de datos en cuanto a los ambientes productivos. Lo anterior, por medio de la funcionalidad nativa de AZURE - Backup Vaults.

Adicional a lo anterior, para las aplicaciones, se tienen contenedores específicos llamados Recovery Vaults los cuales funcionan como bóvedas inmutables para la prevención de ataques y la rápida restauración de la información en caso de ataques o que se vea comprometida la información.

En consecuencia, con lo anterior, la Subdirección de Tecnologías de la Información, ha mitigado el riesgo garantizando la confidencialidad, integridad y disponibilidad de la información. Por tanto, no se acepta esta no conformidad."

Análisis Oficina de Control Interno: la Oficina de Control Interno evidencia que la respuesta dada por el proceso auditado no corresponde a la **No conformidad N°. 5. "***Incumplimiento al ARTICULO 2.2.17.1.6. y al ARTÍCULO 2.2.17.5.6 del decreto 1078 de 2015.***"** al proceso *"Gobierno y Gestión de Datos e Información"* en la actividad *"Gestionar TI"*, liderado por la Dirección de Innovación y Desarrollo y la Subdirección de Tecnología de la Información, plasmada en el informe preliminar con radicado 20241400000127003 del 17 de diciembre de 2024**,** la Secretaria General se pronunció al respecto con radicado 20249000000130443 de 26 de diciembre de 2024 de la **No conformidad N°. 5** en los siguientes términos:

"En atención al memorando en referencia desde la Secretaría General me permito dar respuesta al informe preliminar de Auditoría Interna en los siguientes términos:

- ***No se evidenció actualización del Plan de Continuidad del Negocio de la SNS, la última actualización fue del 2021.***

RTA: Teniendo en cuenta que, el Plan de Continuidad de Negocio busca asegurar que las entidades puedan mantener sus funciones críticas operativas durante y después de un desastre. Este plan se centra en minimizar la interrupción de las operaciones y en asegurar la estabilidad financiera y funcional.

Pese a que este hallazgo ya se había notificado en 2022, no se encontró el Plan de Mejoramiento Formulado ni el seguimiento correspondiente en el año 2023. En tal sentido, consideramos que desde la Oficina Asesora de Planeación se debe liderar la actualización constante del PCN, dado su rol en la planificación estratégica y operacional de la entidad, con el respectivo apoyo de la Dirección de Innovación y Desarrollo, la Subdirección de Tecnologías de la Información y la Secretaría General.

- ***La Entidad no cuenta con procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales.***

RTA: El Plan de Recuperación de Desastres es específico para restablecer rápidamente las funciones y servicios críticos después de una interrupción. Se enfoca en asegurar la continuidad de los sistemas de información y tecnológicos es parte integral del plan de continuidad del negocio. La Dirección de Innovación y Desarrollo y a la Subdirección de Tecnologías de la Información sería la responsable de desarrollar y mantener estos planes actualizados, asegurando que los sistemas informáticos puedan recuperarse rápidamente tras una interrupción.

- ***No se encuentra documentada la actuación frente a las contingencias y no se ha actualizado el plan de contingencia; tampoco se observó algún trámite que se haya adelantado en ese sentido****.*

RTA: Con el liderazgo de la Oficina Asesora de Planeación, en conjunto con la Dirección de Innovación y Desarrollo, la Subdirección de Tecnologías de la Información y la Secretaría General, se debe llevar a cabo la actualización del plan de contingencia. Este proceso incluye la definición de escenarios alternos de operación que permitan asegurar la continuidad de las funciones críticas de la Entidad, tal como se estableció en el BIA.

- ***No se han adelantado las acciones para ajustar y/o mejorar el BIA de la Entidad.***

RTA: El BIA identifica las funciones vitales de la entidad y evalúa el impacto potencial de una interrupción en estas áreas. Ayuda a determinar y priorizar los recursos que deben ser recuperados. La Dirección de Innovación y Desarrollo y a la Subdirección de Tecnologías de la Información serían las responsables de mantener actualizado el BIA, dado que parte del análisis implicaría evaluar cómo las interrupciones en los sistemas de TI afectarían las operaciones de la entidad.

La Oficina Asesora de Planeación también estaría involucrada en el BIA desde una perspectiva más amplia, evaluando cómo diferentes tipos de interrupciones podrían afectar diversas áreas de la organización.

- ***No se tiene definido el plan de contingencias de la Entidad y no han sido socializado a la Entidad tanto a los líderes de procesos como a sus equipos de trabajo***

RTA: Con el liderazgo de la Oficina Asesora de Planeación, en conjunto con la Dirección de Innovación y Desarrollo, la Subdirección de Tecnologías de la Información y la Secretaría General, se debe llevar a cabo la actualización del plan de contingencia. Este proceso incluye la definición de escenarios alternos de operación que permitan asegurar la continuidad de las funciones críticas de la Entidad, tal como se estableció en el BIA.

- ***Debilidad en entrega de cargo por parte de exfuncionarios desde la Secretaría General junto con Talento Humano y la Dirección de Innovación de Desarrollo se permite poner en su conocimiento las actuaciones que se realizan actualmente:***

RTA: Es pertinente resaltar que en el marco del Comité de Gestión y Desempeño Institucional No 63. Del 19 de diciembre de 2024, se presentó y aprobó la Estrategia de Levantamiento, Mapeo y Gestión del Conocimiento con el fin de asegurar el conocimiento en la Superintendencia Nacional de Salud.

Les agradecemos y solicitamos respetuosamente tener en cuenta estas consideraciones dentro del informe final de auditoría."

La Oficina de Control Interno con Fundamento a lo expuesto por la Secretaria General frente a la **No conformidad N°. 5**, se recategoriza el hallazgo a **Observación N°. 11 "*Debilidad en el cumplimiento al ARTICULO 2.2.17.1.6. y al ARTÍCULO 2.2.17.5.6 del decreto 1078 de 2015***", por lo expuesto se insta a que se realice la actualización del plan de continuidad del negocio con su correspondiente BIA y el plan de contingencia que corresponda a la estructura organizacional, Así mismo documentar de manera estructurada todos los procedimientos, guías, tramites y socialización o capacitaciones y documentar todas las acciones adelantadas por la entidad con respecto a simulacros, incidentes y planes de contingencia, y así lograr mitigar de manera acertada la materialización de riesgos, garantizar los recurso tanto humanos, técnicos, económicos y con los cuales se podría generar una base de conocimientos para garantizar la integridad, confidencialidad y la disponibilidad de los sistemas de información y de infraestructuras físicas y tecnológicas de la SNS, situación que configurará seguimiento posterior por parte de la Oficina de Control Interno.

No conformidad N°. 6. Incumplimiento en el diligenciamiento Mapa de Riesgos de Seguridad y Privacidad de la Información – DEFT24

Respuesta del proceso auditado con radicado 20241530400130463 de 26 de diciembre de 2024:

NO CONFORMIDAD No. 6 - Incumplimiento en el diligenciamiento Mapa de Riesgos de Seguridad y Privacidad de la Información – DEFT24, a los procesos "Gobierno y Gestión de Datos e información", liderado por la Dirección de Innovación y desarrollo, y; "Direccionamiento Estratégico" actividad calve de éxito "Gestionar Riesgos", liderado por la Oficina Asesora de Planeación

"Actualmente se encuentra en proceso de actualización de los procedimientos del grupo de seguridad digital, con el fin de ajustar los riesgos del mismo, de manera que se pueda cerrar dicha actividad.

Se inicia la identificación de riesgos de seguridad y privacidad de la información con capacitaciones y mesas de trabajo a los gestores de la entidad, se publicará la matriz de riesgos de seguridad y privacidad de la información en su primera versión con los procesos actuales de la entidad a finales del mes de enero de 2025.

En el desarrollo del plan de seguridad 1452 con tres actividades (identificación, actualización y publicación), y su fecha de culminación es el 20 de enero de 2025.

Se realiza la actualización y publicación, junto a la OAP, del manual de administración del riesgo - DEMN02 de la entidad."

Análisis Oficina de Control Interno: la Oficina de Control Interno evidencia que la respuesta dada por el proceso auditado no corresponde a la ***No conformidad N°. 6. "Incumplimiento en el diligenciamiento Mapa de Riesgos de Seguridad y Privacidad de la Información – DEFT24"*** a los procesos "*Gobierno y Gestión de Datos e información*", liderado por la Dirección de Innovación y desarrollo, y; "*Direccionamiento Estratégico*" actividad calve de éxito "*Gestionar Riesgos*", liderado por la Oficina Asesora de Planeación, plasmada en el informe preliminar con radicado 20241400000127003 del 17 de diciembre de 2024**,** motivo por el cual se ratifica la **No conformidad N°. 6**, situación que configurará seguimiento posterior por parte de la Oficina de Control Interno.

5 CONCLUSIONES

El auditor de la Oficina de Control Interno pudo concluir el cumplimiento del objetivo propuesto por la auditoría, consistente en establecer el grado de conformidad de la gestión emprendida por parte de los procesos "*Gobierno y Gestión de Datos e Información*" y "*Gestión de Bienes y Servicios*", A través del presente informe, la oficina de Control Interno pone en consideración de la Alta Dirección institucional, que se adelanten las acciones necesarias que permita apoyar con los recursos humanos, técnicos – económicos para fortalecer el Sistema de Seguridad y Privacidad de la Información de la SNS, así mismo que sirva para tomar las decisiones que permitan el mejoramiento continuo de estos procesos institucionales.

Se identificó que el proceso de "*Gobierno y Gestión de Datos e Información*" no cuenta con una debida transferencia de conocimiento y una base de conocimiento que contenga los documentos, procedimientos, actividades, informes técnicos, Gestión de incidentes, lecciones aprendidas y todo lo relacionado con las políticas de Gobierno y Seguridad Digital.

Es importante que las Entidad conozca de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital.

Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo

establece el MIPG. Por consiguiente, se debe incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.

En términos generales puede indicarse que, los procesos auditados operan y se gestionan en un ambiente de control al contarse estos con riesgos identificados, el establecimiento de controles y acciones de tratamiento que contribuyen a mitigarlos, indistintamente de las oportunidades de mejoramiento documentadas

Las recomendaciones y hallazgos (conformidades, observaciones y no conformidades) que por medio del presente informe se exponen, se formulan en ejercicio del rol de "*Enfoque hacia la prevención*" legalmente asignado a las Oficinas de Control Interno, a través del Decreto 648 de 2017, con el fin precaver situaciones que puedan continuar afectando los procesos objeto de evaluación y afianzar los aspectos que se detectaron como conformes, lo cuales serán objeto de seguimiento por la Oficina de Control Interno.

Las recomendaciones y hallazgos (conformidades, observaciones y no conformidades) que por medio del presente informe se exponen, se formulan en ejercicio del rol de "Enfoque hacia la prevención" legalmente asignado a las Oficinas de Control Interno, a través del Decreto 648 de 2017, con el fin precaver situaciones que puedan continuar afectando los procesos objeto de evaluación y afianzar los aspectos que se detectaron como conformes.

Finalmente, de acuerdo con lo expuesto en el presente informe final, los hallazgos detectados se identificaron como: "una (1) conformidades, once (11) observaciones y cinco (5) No Conformidades", los cuales serán incorporados en el Aplicativo de Planeación y Gestión (ITS), por lo que la Oficina de Control Interno solicita a los líderes responsables de realizar los planes de mejoramiento, que una vez se reciban las respectivas notificaciones en el referido aplicativo, se dé trámite a la formulación de los Planes de Mejoramiento a que haya lugar, tal como lo dispone la actividad clave de éxito "Ejecutar Plan de Mejoramiento", donde se establece que "Analizar los hallazgos y proceder a definir su tratamiento.

El líder del proceso, programa o proyecto, luego de recibir la alerta del cargue de los hallazgos en el sistema dispuesto por la entidad, dispone de **10 días hábiles** para identificar la acción o tratamiento de mejora a aplicar.", los cuales estarán encaminados a subsanar las situaciones evidenciadas y a los que la Oficina de Control Interno realizará seguimiento posterior. Negrillas Extratextuales.

Cordialmente,

Jorge Alejandro Cárdenas Leuro
Jefe Oficina de Control Interno (e)

Proyectó: Juan Carlos Nocua Camargo, Auditor Líder.
Revisó y aprobó: Jorge Alejandro Cardenas Leuro, Jefe Oficina de Control Interno (e)