Informe Ejecutivo auditoría a los sistemas de información de la SNS	**Día**	**25**	**Mes**	**octubre**	**Año**	**2023**
Informe detallado dirigido a:	Superintendente Nacional de Salud Comité Institucional de Coordinación de Control Interno - CICCI					
Informe Ejecutivo dirigido a:	Publicación página web					
Procesos auditados	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.					
Objetivo	Establecer el grado de conformidad de los sistemas de información de la Superintendencia Nacional de Salud, evaluando la aplicabilidad de los principios de seguridad, confidencialidad, integridad y disponibilidad que les aplican. Las actividades generales del presente ejercicio auditor son: 1. Evaluar los Sistemas de información seleccionados por muestreo, posterior a las pruebas de recorrido iniciales, validando lo siguiente: ▪ Niveles de acceso de usuarios. ▪ Entrada-proceso-salida de información. ▪ Reportes y consultas. ▪ Copias de seguridad de cada sistema. ▪ Seguridad, confidencialidad, integridad y disponibilidad de los sistemas de información seleccionados. 2. Continuidad del negocio, plan de contingencia de la entidad, seguridad de la información y actualización de procesos y procedimientos relacionados con el tema. Seguimiento a informes anteriores respecto de este tema. 3. Verificar proyectos de inversión relacionados con el objeto de la auditoría. 4. Verificar la ejecución contractual a cargo de la Subdirección de Tecnologías de la Información (precontractual, contractual y post contractual), de acuerdo con la muestra seleccionada, 5. Verificar cumplimiento de lo establecido en la Resolución 2021160000013752–6 del 28 de octubre de 2021 por la cual se establecen las reuniones de autoevaluación. 6. Verificar cumplimiento y efectividad de los controles definidos en el mapa de riesgos institucional (riesgos de gestión, corrupción y seguridad digital). 7. Seguimiento a los hallazgos identificados en diferentes informes presentados durante la vigencia 2022 y primer semestre de 2023.					
Alcance	Seguridad de la información en los sistemas de información seleccionados según muestreo. En términos de tiempo, la auditoría abarca el periodo comprendido entre el 01/07/2022 y el 30/07/2023.					
Tabla de Contenido						
Equipo Auditor	Eddna Dueñas Monsalve, profesional especializado Oficina de Control Interno Peter William Vargas Pinilla, profesional especializado Oficina de Control Interno					
Jefe Oficina de Control Interno (e)	Consuelo Eugenia Vélez Tobón					

La auditoria a los sistemas de información se realizó a una muestra seleccionada de nueve (9) aplicativos a saber:

- Bpm
- Fenix
- Gaudi
- Humano
- Nrvcc
- Página Web e Intranet
- Rilco
- Siad
- Sivical

➢ En los sistemas seleccionados, se realizaron validaciones respecto de:

- Acceso y perfiles de usuarios (administradores, técnicos y funcionales).
- Entrada-proceso-salida de información.
- Reportes y consultas.
- Copias de seguridad y restauración.
- Aplicación de la seguridad, confidencialidad, integridad y disponibilidad

De acuerdo a las pruebas de recorrido realizadas y la información y evidencias aportadas por la Dirección de Innovación y Desarrollo, Subdirección de Tecnologías de la Información, Dirección de Contratación, Dirección de Talento Humano y una vez analizadas por el equipo auditor frente al objetivo y alcance de la auditoría, se determinaron los siguientes hallazgos:

1. Resumen ejecutivo de los hallazgos determinados en el informe final de auditoría

Hallazgo	N°	Título del Hallazgo
Conformidad	2.1.1	Adecuada ejecución proyectos de inversión asignados durante la vigencia 2022.
Observación	2.2.1	Debilidad en la formalización de entrega de cargos de exfuncionarios de la DID y la STI
Observación	2.2.2	Debilidad en la aplicación de controles relacionados con políticas de seguridad
Observación	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"
Observación	2.2.4	Debilidad en seguimiento a las acciones determinadas en Puestos de Mando Unificados.
Observación	2.2.5	Falta de definición y aprobación de documentos sobre "Roles y responsabilidades", "manual de Seguridad de la información".
Observación	2.2.6	Debilidad en el monitoreo y análisis de vulnerabilidades a los sistemas de información, servidores e infraestructura de la entidad.

Hallazgo	N°	Título del Hallazgo
Observación	2.2.7	Debilidad en la verificación de la actualización de antivirus, firewall y sistemas operativos de los servidores de las aplicaciones.
Observación	2.2.8	Debilidad en la implementación de un documento que especifique los lineamientos para la realización de copias de seguridad, tiempo de retención y plan de recuperación de copias.
Observación	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.
Observación	2.2.10	Oportunidad de mejora en la ejecución de proyectos de inversión año 2023 de la DID - STI
Observación	2.2.11	Debilidad en la supervisión del contrato 158 de 2022.
Observación	2.2.12	Debilidad en el reporte de materialización de riesgos, por parte de la STI
Observación	2.2.13	Falta de oportunidad en la generación de informes de monitoreo de los riesgos de seguridad y privacidad de la información.
No Conformidad	2.3.1	No se cuenta con una matriz de roles y responsabilidades y de segregación de funciones.
No Conformidad	2.3.2	Materialización de riesgos de seguridad de la información, por vulneración de los principios de “Confidencialidad, Integridad y Disponibilidad”, así mismo la materialización de riesgos de gestión definidos para la vigencia 2023.
No Conformidad	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”.
No Conformidad	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”
No Conformidad	2.3.5	Incumplimiento de las políticas del componente de Seguridad de la Información y Seguridad Digital “respaldo de la información”.
No Conformidad	2.3.6	Debilidad en el cumplimiento de la Resolución 2021160000013752-6 del 28/10/2021 “Por la cual se adoptan las reuniones de autoevaluación en la SNS”.

2. Conclusiones del informe final de auditoría

De acuerdo con la muestra seleccionada, las pruebas realizadas y la información aportada, el equipo auditor concluye que:

- De acuerdo con las evidencias aportadas, el equipo auditor de la Oficina de Control Interno evidenció debilidades en los siguientes aspectos, que determinaron Observaciones y No Conformidades, que se relacionan en el **numeral 2º** del informe detallado:

  - ✓ Debilidad en la aplicación de controles relacionados con políticas de seguridad.
  - ✓ La entidad no cuenta con una metodología estructurada para la atención de incidentes de seguridad de la información.
  - ✓ La entidad no cuenta con un plan de continuidad del negocio actualizada.

- ✓ La entidad no cuenta con un plan de contingencia, ni un plan de recuperación de desastres o incidentes".
- ✓ Se evidenció debilidad en el monitoreo y análisis de vulnerabilidades a los sistemas de información, servidores e infraestructura de la entidad
- ✓ Se evidenció debilidad en la verificación de la actualización de antivirus, firewall y sistemas operativos de los servidores de las aplicaciones.
- ✓ Se evidenció 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.
- ✓ Se evidenció que no se han definido 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.
- ✓ Se evidenció debilidad en la supervisión del contrato 158 de 2022.
- ✓ La Entidad no cuenta con una matriz de roles y responsabilidades y de segregación de funciones.
- ✓ Se materializaron riesgos de seguridad de la información, por vulneración de los principios de "Confidencialidad, Integridad y Disponibilidad".
- ✓ Se evidenció incumplimiento de los siguientes lineamientos definidos en el Manual de Políticas Institucionales FIMN07 (ahora DEFT13):
  - La revisión de los riesgos de Seguridad de la Información y Seguridad Digital se llevará a cabo como mínimo una vez al año.
  - Control de accesos / gestión de contraseñas
  - Respaldo de la información.
- ✓ Se evidenció que la DID y la STI, no han realizado acciones claras y concretas para subsanar los hallazgos representados en informes de auditorías y de seguimientos presentados por la OCI, en periodos anteriores (vigencias 2022 y 2023)
- ✓ Se evidenció debilidad en el cumplimiento de la Resolución 2021160000013752-6 del 28/10/2021 "Por la cual se adoptan las reuniones de autoevaluación en la Superintendencia Nacional de Salud".

➢ De acuerdo con las evidencias aportadas, **es importante que se defina un modelo de gestión de incidentes de seguridad de la información** que incluya aspectos como 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, en las que se contemple por lo menos:

1. Activar protocolos de atención de incidentes de seguridad y ciberseguridad.
2. Analizar la situación o suceso de seguridad.

3. Realizar monitoreos periódicos con sus correspondientes soportes, que permitan definir una línea base para cuando se presente un incidente.
4. Definir el equipo de detección y respuesta ante incidentes de seguridad, donde se establezcan:
    a. Roles y responsabilidades (incluyendo a la alta dirección – PMU).
    b. Segregar adecuadamente funciones, tanto técnicas, operativas y funcionales.
    c. Plan de acción o plan de choque para apoyar a las dependencias que tuvieren afectación.
    d. Seguimiento a los compromisos derivados de cada reunión del PMU.
    e. Seguimiento y verificación de resultados de las investigaciones adelantadas con respecto al incidente (denuncias internas y externas).
5. Mantener actualizados los sistemas de información e infraestructuras:
    a. Realizar **análisis de vulnerabilidades** periódicamente, que estén documentados y que se realicen las acciones correspondientes para corregir las situaciones o reducir el impacto en la posible materialización de riesgos.
    b. Definir y fortalecer las **herramientas de seguridad** de la información
    c. Garantizar la disponibilidad de las **copias de seguridad** de los aplicativos, bases de datos, servidores, etc.
    d. Revisión periódica y documentada respecto de la **infraestructura** de la entidad (cableado estructurado, conexión con puntos remotos-Regionales, etc.)
    e. Realizar los mantenimientos que sean necesarios para evitar la obsolescencia de sistemas, servidores, infraestructura, entre otros, lo cual redundará en conservar de manera adecuada los históricos de la información (memorial institucional).
    f. Garantizar que **los ambientes de** desarrollo, pruebas y producción se encuentren separados y en óptimas condiciones para cuando se requiera atender un incidente y recurrir a ellos para garantizar la continuidad de las operaciones, sin mayores impactos.
    g. Asegurar las **plataformas y los servicios** de la entidad (parches, antivirus, firewall, actualizaciones de sistema operativo en servidores, restricciones de acceso a páginas web sospechosas, etc.)
6. Implementar políticas de **seguridad** y **ciberseguridad**
    a. Actualizar las políticas de seguridad de la información.
    b. Monitorear usuarios y accesos.
    c. Actualizar contraseñas a intervalos de tiempos periódicos y razonables.
    d. Actualizar mapa de riesgos de seguridad y privacidad de la información.
    e. Proyectar planes de tratamiento de riesgos cuando se determine la materialización de riesgos (disponibilidad, integridad, confidencialidad, entre otros).
    f. Ejecutar actividades de pruebas de seguridad (Ethical Hacking) periódicas y documentarlas.
    g. Realizar periódicamente la depuración de usuarios, perfiles, permisos.

h. Configurar 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.

7. **Contar con el personal experto, idóneo y calificado** para la administración de herramientas, aplicaciones, servidores, infraestructura, bases de datos, etc., para lo cual es pertinente contar con el apoyo de las instancias pertinentes al interior de la entidad.
8. Adoptar buenas prácticas de administración, monitoreo y gestión.
9. Dar cumplimiento a modelos de gestión (por ejemplo, normas ISO 27001 y sus derivadas; 31001 y sus derivadas, 22301, entre otras), o lineamientos determinados por entidades como el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y del Departamento Administrativo de la Función Pública -DAFP, entre otras.

En todas las situaciones que se acaban de detallar, es pertinente que se establezca la documentación necesaria que las debe soportar, lo cual permite tener una base de conocimiento para la atención de eventos / incidentes, o incluso para cuando se presenta alta rotación de personal, exigiendo la correspondiente transferencia de conocimiento y entrega de cargos de manera formal y oficial.

- De acuerdo con la verificación contractual realizada, se coligen debilidades en la supervisión del contrato analizado, toda vez que el Supervisor certificó el cumplimiento de las obligaciones del contratista, sin dejar relacionado el detalle de las verificaciones efectuadas y sus resultados, en los informes correspondientes, 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; así mismo se evidenció la falta de publicidad de los pagos e informes de supervisión en “Colombia Compra Eficiente”.

- Durante lo corrido de la vigencia 2023 los sistemas de información verificados, tuvieron problema de disponibilidad y uno (1) de ellos tuvo pérdida de información (SIAD), la cual fue recuperada según plan de choque diseñado por la Superintendencia Delegada de Investigaciones Administrativas (SDIA), tomando información de los expedientes físicos y de las notificaciones electrónicas efectuadas por el sistema SuperArgo, información reportada a la DID para actualizar el sistema.

- De la trazabilidad de información aportada por la SDIA respecto de la afectación del sistema SIAD, se observa falta de oportunidad en la atención que se debió brindar por el área técnica para la recuperación de la información o en su defecto, la definición de una herramienta que permita a esa Delegatura consolidar la información de trazabilidad de los expedientes, lo que ha generado retrasos y reprocesos teniendo que establecer un plan de choque para recurrir a los expedientes físicos y reconstruir la información que contenía SIAD.

- Como resultado de la auditoría, se identificaron una (1) Conformidad, trece (13) Observaciones y seis (6) No Conformidades enunciadas en el numeral anterior.

- De acuerdo con la estructura institucional definida mediante Decreto 1080 de 2021, los procesos relacionados en la matriz de riesgos institucional que se verificó no existen o cambiaron de nombre y se convirtieron en actividades claves de éxito de otro proceso padre, como se relaciona a continuación:

Nombre del proceso según Decreto 2462 de 2013	Nombre del proceso según Decreto
Provisión de soluciones tecnológicas	*Gobierno y Gestión de Datos e Información*
Gestión de Servicios Tecnológicos	*Gobierno y Gestión de Datos e Información*
Gestión del Procedimiento Administrativo	Control

Tabla N. 63. Fuente: Construcción propia Oficina de Control Interno

Por lo anterior, los hallazgos determinados en esta auditoría se registrarán en el sistema ITS, al proceso ***Gobierno y Gestión de Datos e Información*** liderado por la Dirección de Innovación y Desarrollo, el cual asumió los procesos que con la anterior estructura lideraba la Oficina de Tecnologías de la Información ahora Subdirección de Tecnologías de la Información.

Cordialmente,

CONSUELO EUGENIA VÉLEZ TOBÓN
Jefe Oficina de Control Interno (e)

Elaboró: Eddna Dueñas Monsalve
Profesional Especializada de la OCI