Supersalud	GOBIERNO Y GESTIÓN DE DATOS E INFORMACIÓN	CÓDIGO	DIMN22
	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN	1
		FECHA	02/03/2026

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Superintendencia Nacional de Salud

Fecha del documento (02 – 03 – 2026)

Supersalud

1. OBJETIVO

Establecer la política general del Sistema de Gestión de Seguridad de la Información y sus políticas específicas, así como definir los lineamientos frente al uso y manejo de la información que deben conocer y cumplir todos los funcionarios, contratistas y partes interesadas de la Superintendencia Nacional de Salud.

2. ALCANCE

La Superintendencia Nacional de Salud gestiona, controla y salvaguarda la confidencialidad, integridad y disponibilidad de la información de los procesos de la Entidad mediante la gestión de riesgos de seguridad de la información y la implementación de controles físicos y digitales para prevenir incidentes, promover la continuidad de las operaciones y desarrollar la cultura de seguridad de la información.

De igual manera, pretende cumplir con la normatividad vigente y otras disposiciones en el marco de la mejora continua del mencionado sistema.

3. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.1. Objetivo General:

La Superintendencia Nacional de Salud entiende y reconoce la dependencia y vulnerabilidad derivada del uso de las tecnologías de la información, así como la importancia de garantizar tanto la **seguridad de la información** como la **privacidad y protección de los datos personales**. Para ello, establece políticas que aseguren la **confidencialidad, integridad y disponibilidad** de la información institucional, al tiempo que garantizan el respeto de los **derechos de los titulares de datos**

personales, la gestión responsable de los riesgos asociados al tratamiento de información, y el cumplimiento de las disposiciones legales en materia de **protección de datos personales**.

La Superintendencia Nacional de Salud declara su compromiso de implementar, operar y mejorar de forma continua el **Sistema de Gestión de Seguridad y Privacidad de la Información**, aplicando los lineamientos establecidos y publicados, acorde con las necesidades misionales de la entidad. Este sistema integra la gestión de ciberseguridad, el aseguramiento de los datos personales, la protección de la privacidad y la continuidad en la operación de los servicios que la Superintendencia presta.

3.2. Objetivos Específicos:

- Identificar y gestionar los riesgos de seguridad y privacidad de la información, con el fin de preservar la confidencialidad, integridad y disponibilidad de los datos, así como proteger los derechos fundamentales de los titulares.
- Definir y establecer controles técnicos, jurídicos y organizacionales que prevengan la materialización y mitiguen el impacto de los riesgos que puedan afectar la seguridad de la información y la privacidad de los datos personales.
- Proteger y asegurar los activos de información y las bases de datos personales, garantizando la aplicación de controles que preserven su confidencialidad, integridad, disponibilidad y uso legítimo conforme a la normativa de protección de datos personales.
- Desarrollar y fortalecer una cultura institucional de seguridad y privacidad, promoviendo el conocimiento, la sensibilización y la responsabilidad de servidores públicos, contratistas y terceros frente a la protección de la información y los derechos de los titulares de datos personales.

- Establecer un marco de referencia institucional integral, que contemple la seguridad de la información, la ciberseguridad, la protección de datos personales y la privacidad como elementos interdependientes de la gestión pública.
- Gestionar de manera oportuna y estandarizada los incidentes de seguridad y las vulneraciones de datos personales, con el fin de mitigar los posibles impactos, dar cumplimiento a las obligaciones legales de reporte y garantizar la atención adecuada de los titulares afectados.
- Generar y mantener la confianza de los ciudadanos, servidores públicos y partes interesadas en el manejo seguro, legítimo y transparente de la información y los datos personales confiados a la Superintendencia.
- Establecer y aplicar políticas, procedimientos e instructivos en materia de seguridad y privacidad de la información, incorporando los criterios correspondientes en los documentos, procesos y servicios de la entidad.
- Garantizar la aplicación de buenas prácticas en continuidad del negocio, gestión del cambio, gestión de accesos, gestión del riesgo y gestión de incidentes, integrando de forma transversal los principios de privacidad y protección de datos personales.

3. NORMATIVIDAD

Ley 1266 de 2008 “por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.” La Entidad cumplirá con los deberes y responsabilidades para garantizar la protección de los derechos del titular de los datos, en la información proveniente de terceros.

Decreto Ley 1151 de 2008 “Establecen los lineamientos generales de la estrategia de gobierno en línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

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

Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales.” La Superintendencia deberá aplicar los principios sobre protección de datos en todas y cada una de las bases de datos que gestione la Entidad.

Decreto 2364 de 2012, “Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.”

Decreto 2462 de 2013 “Por medio del cual se modifica la estructura de la Superintendencia Nacional de Salud” En el artículo 11 se establecen las funciones que debe cumplir la Oficina de Tecnologías de la Información para el cumplimiento de los objetivos estratégicos de la Entidad.

Decreto 2573 de 2014, “Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en Línea, se reglamenta parcialmente, la Ley 1341 de 2009 y se dictan otras disposiciones”

Decreto 1078 DE 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”

Decreto 415 DE 2016, “por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones”

Resolución MINTIC 02893 de 2020, “Por la cual se expiden los lineamientos para

estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones"

Decreto 088 del 2021, "(…) digitalización y automatización de trámites y su realización en línea"

Directiva Presidencial 03 de 2021, Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión

Resolución MINTIC 0500 del 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"

Resolución MINTIC 460 de 2022, Se expide el Plan de Infraestructura de Datos y su hoja de ruta.

Directiva Presidencial 02 de 2022, Reiteración Política Pública en materia de Seguridad Digital

Decreto 767 del 2022, Mediante el cual se realiza la actualización Política Colombiana de Gobierno Digital

Decreto 338 del 2022, lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

Resolución MINTIC 0746 del 2022, Se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales.

Resolución MINTIC 002227 del 2025, Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

4. TERMINOS Y DEFINICIONES

Activo de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. [Modelo de Seguridad y Privacidad de la Información 3.0.2].

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. [ISO/IEC 27000:2018].

Auditoría: Inspección formal para verificar si se está siguiendo/cumpliendo un estándar o un conjunto de guías, que sus registros son precisos o que las metas de eficiencia y efectividad se están cumpliendo. [ITIL® Español (España) glosario, v1.0].

ITIL: Information Technology Infrastructure Library Biblioteca de Infraestructura de Tecnologías de la Información para la gestión de servicios de TI (IT Service Management, ITSM).

ISO: International Organization for Standardization (Organización Internacional de Normalización. estándares internacionales que establecen requisitos y buenas prácticas en distintos ámbitos (calidad, medio ambiente, seguridad, tecnología, etc.).

IEC:International Electrotechnical Commission (Comisión Electrotécnica Internacional). que establecen criterios de diseño, seguridad, compatibilidad y desempeño para sistemas y componentes eléctricos y electrónicos.

ISO/IEC 27000:2018: Norma Internacional que sirve como introducción y glosario para toda la familia de normas ISO/IEC 27000, diccionario y la guía básica de la serie de normas sobre seguridad de la información.

Confidencialidad: Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.

Continuidad del Negocio: Procedimientos y/o procesos para asegurar la continuidad de las operaciones del negocio. [ISO/IEC 27000:2018].

Control: Medios de gestión del riesgo, incluidas las políticas, procedimientos, directrices, prácticas y estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o jurídico. [ISO/IEC 27000:2018].

Copia de seguridad: Copiar los datos para proteger los originales de pérdidas de integridad o disponibilidad. [ITIL® Español (España) glosario, v1.0].

Disponibilidad: Es la garantía de poder acceder a los activos de la información cuando sea necesario, por personal autorizado.

Dispositivo móvil: Elemento electrónico de tamaño pequeño, con capacidades de procesamiento de datos, conexión a Internet y memoria Son ejemplos de estos: celulares inteligentes, tabletas y portátiles.

El Teletrabajador: es la persona que el marco de la relación laboral dependiente utiliza las tecnologías de la información y comunicación como medio o fin para realizar su actividad laboral fuera del local del empleador, en cualquiera de las formas definidas por la ley.

Evento de Seguridad de La información: Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

Firewall: Dispositivo que permite bloquear o filtrar el acceso en redes de comunicación.

Firma Digital: La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Funcionarios: Las personas naturales que ejercen la función pública

establecen una relación laboral con el estado y son en consecuencia funcionarios públicos.

Gestión de accesos: Proceso responsable de permitir a los usuarios hacer uso de los servicios de TI, datos u otros activos. [ITIL® Español (España) glosario, v1.0].

Gestión de activos: Es una actividad genérica o proceso responsable del seguimiento y la notificación del valor y la propiedad de los activos a lo largo de su ciclo de vida. [ITIL® Español (España) glosario, v1.0].

Gestión de la capacidad: Proceso responsable de asegurar que la capacidad de los servicios de TI y de la infraestructura de TI puedan cumplir con los requerimientos acordados, relacionados con la capacidad y el rendimiento de una manera rentable y a tiempo. [ITIL® Español (España) glosario, v1.0].

Gestión de cambios: Proceso responsable del control del ciclo de vida de los cambios, permitiendo la ejecución de los cambios beneficiosos minimizando el impacto en los servicios de TI. [ITIL® Español (España) glosario, v1.0].

Incidente de seguridad: Evento único o serie de eventos de seguridad de la información inesperada o no deseado que posean una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000:2018].

Infraestructura de TI: Todo el hardware, software, redes, instalaciones etc. requeridas para desarrollar, probar, proveer, monitorizar, controlar o soportar aplicaciones y servicios de TI. [ITIL® Español (España) glosario, v1.0].

Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. [ISO/IEC 27000]

Información Pública: Aquella que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. [Ley N° 1712, 2014, Glosario].

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014. [Ley N° 1712, 2014, art. 6°. Definiciones, literal c].

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la 9: Libertad y Orden ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014. [Ley N° 1712, 2014, art. 6°. Definiciones, literal d].

Integridad: Propiedad de exactitud y completitud de la información. [ISO/IEC 27000:2012].

Internet: El sistema único, interconectado, mundial de redes informáticas comerciales, gubernamentales, educativas y de otro tipo que comparten (a) el conjunto de protocolos especificado por Internet Architecture Board (IAB) y (b) los espacios de nombres y direcciones administrados por Internet Corporation para Nombres y Números Asignados (ICANN). [CSRC NIST].

ICANN: (Corporación de Internet para la Asignación de Nombres y Números). organización que asegura que cuando escribes una dirección web (como *www.microsoft.com*), tu computadora pueda encontrar el servidor correcto en cualquier parte del mundo

CSRC NIST: Computer Security Resource Center del NIST (National Institute of Standards and Technology de Estados Unidos). Es un portal oficial del NIST dedicado a la ciberseguridad y seguridad de la información.

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa

del estado, con el fin de identificar cambios respecto al nivel de desempeño exigido o esperado. [ISO/IEC 27000:2018].

Parte interesada: Persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad. [ISO/IEC 27000:2018]

Política: Intención y dirección generales expresadas formalmente por la Dirección. [ISO/IEC 27000:2018].

Procedimiento: Manera especificada de llevar a cabo una actividad o un proceso. [ISO/IEC 27000:2018].

Prueba: Una actividad que verifica que un elemento de configuración, servicio de TI, proceso, etc. cumple con sus especificaciones o requerimientos acordados. [ITIL® español (España) glosario, v1.0].

Revisión: Actividad emprendida para determinar la idoneidad, adecuación y efectividad de la materia para alcanzar los objetivos establecidos. [ISO/IEC 27000:2012].

Riesgo: Efecto de la incertidumbre sobre los objetivos. [ISO/IEC 27000:2018].

Recursos Físicos: Hace referencia, pero sin limitarse a los hardware susceptibles de actualizaciones de seguridad y/o modificaciones funcionales y no funcionales pertenecientes a la Superintendencia Nacional de Salud o en su defecto en modalidad de arriendo y/o de terceros que presten servicios a la entidad.

Recursos Lógicos: Hace referencia, pero sin limitarse a los sistemas de información, derivados y/ componentes susceptibles de actualizaciones de seguridad y/o modificaciones funcionales y no funcionales pertenecientes a la Superintendencia Nacional de Salud o en su defecto de terceros que presten servicios a la entidad.

Servidor: Ordenador que está conectado a la red y que provee funciones de software que son usadas por otros ordenadores. [ITIL® Español (España) glosario, v1.0].

Seguridad de la información: Preservación de confidencialidad, integridad y disponibilidad de la información. [ISO/IEC 27000:2018].

Usuario externo: Son todos los terceros interesados que utilizan información y servicios tecnológicos.

Usuario interno: Servidores públicos, contratistas, pasantes y judicantes que utilizan información y servicios tecnológicos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas. [ISO/IEC 27000:2018].

5. POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. Política General de Seguridad de la Información.

La Superintendencia Nacional de Salud se compromete a implementar, fortalecer y mantener su Seguridad Digital y Seguridad de la Información mediante un enfoque integral que garantice la confidencialidad, integridad y disponibilidad de la información institucional, articulando un marco normativo, técnico y operativo que promueva la gestión responsable y proactiva de los riesgos de Seguridad Digital, adoptando controles organizacionales y tecnológicos, fomentando una cultura de seguridad en toda la entidad a través de la capacitación a su talento humano.

5.2. Política de organización interna.

La Superintendencia busca la articulación o coordinación de los procesos estratégicos, misionales y de apoyo para asegurar la información en un escenario de corresponsabilidad. La Subdirección de Subdirección de Tecnologías de la Información (en adelante STI) tiene la responsabilidad de:

- Establecer los roles y responsabilidades para asegurar la información, en

articulación con los diferentes procesos que la gestionan.

- Generar y mantener actualizado un listado de contactos, autoridades y grupos de interés de seguridad de la información para gestionar eficientemente las diferentes actividades de Seguridad de la información
- Apoyar en identificar, evaluar y tomar acciones para mitigar los riesgos en los proyectos y operaciones que impacten la información de los procesos y de la misionalidad de la Superintendencia.

5.3. Política de dispositivos móviles y trabajo en casa.

Se debe garantizar que la información de la Superintendencia Nacional de Salud maneje en condiciones seguras desde dispositivos móviles o fuera de las instalaciones de la Entidad. Por lo tanto, se establece que:

- Es responsabilidad de la STI en articulación con la Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional divulgar las recomendaciones sobre el uso de servicios informáticos en las instalaciones y bajo la modalidad de trabajo en casa.
- De igual manera, es responsabilidad de los usuarios que manejan información de la Superintendencia a través de dispositivos móviles utilizados en la modalidad de trabajo en casa, seguir los siguientes lineamientos:
    - Participar en las jornadas de sensibilización en seguridad y privacidad de la información.
    - Actualizar periódicamente las contraseñas.
    - Conocer y aplicar los procedimientos de seguridad de la información.
    - Usar software licenciado y autorizado por la STI en los equipos de cómputo proporcionados por la Entidad.

- Usar las herramientas dispuestas y/o aprobadas por la STI para el manejo de la información sensible de la Entidad.
- Firmar el acuerdo de confidencialidad de la información para el acceso y uso de la información sensible de la Entidad.
- Dar buen uso del servicio de correo electrónico, mensajería, video conferencia, repositorios de almacenamiento e intercambio de información y acceso a la red (VPN) proporcionado por la Entidad.

5.4. Política de seguridad de los recursos humanos.

Los funcionarios, contratistas y/o colaboradores deben ser conscientes de sus responsabilidades frente al aseguramiento de la información. Por lo anterior, se establece que la Entidad debe contratar el personal idóneo con el propósito de asegurar la comprensión sobre su responsabilidad respecto a las políticas y lineamentos en materia de seguridad de la información. Esto para reducir los riesgos de hurto, fraude, filtraciones o uso inadecuado de la información en los equipos empleados en su tratamiento. Lo anterior, según los siguientes lineamientos:

- La Dirección de Talento Humano debe verificar la documentación sobre los antecedentes, las referencias laborales y los soportes de experiencia del personal en procesos de selección para vacantes de planta.
- La Dirección de Contratación debe verificar los antecedentes, las referencias laborales y los soportes de experiencia relacionada del contratista.
- Todos los funcionarios, contratistas y colaboradores deben reportar a través de los canales definidos por la Entidad, cualquier caso de fuga, modificación no autorizada o pérdida de información sensible que se encuentre almacenada en el equipo de cómputo.
- El funcionario, contratista o colaborador es responsable de la información

que produzca u obtenga, así como de los recursos tecnológicos y de software asignados por la Entidad.

- Los funcionarios, contratistas y colaboradores con relación contractual a través de terceros deben conocer y aplicar las políticas, lineamientos, procedimientos y recomendaciones de seguridad de la información de la Entidad.
- La Entidad debe garantizar que los funcionarios y contratistas sean entrenados y sensibilizados en temas de seguridad y privacidad de la información de manera permanente.
- No está permitido para ningún usuario realizar actividades tales como: borrar, alterar o eliminar información de la Entidad de manera no controlada o sin autorización, de tal forma que se afecte la operación de la Superintendencia.
- Los funcionarios, contratistas y colaboradores de la Superintendencia deben usar los activos de la Entidad, únicamente para el cumplimiento de sus funciones en el marco de la misión institucional.
- Los funcionarios, contratistas y colaboradores de la Superintendencia no deben divulgar la información clasificada o reservada, en lugares públicos o privados mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la Entidad.
- Los funcionarios, contratistas y colaboradores de la Entidad deben asistir a los escenarios de sensibilización en seguridad de la información cuando sean requeridos.
- Es responsabilidad de los usuarios realizar copia de respaldo de la información sensible para la Entidad almacenada en equipos de cómputo o dispositivos móviles teniendo en cuenta los mecanismos de almacenamiento dispuestos por la STI.
- Los funcionarios, contratistas y colaboradores de la Superintendencia no

deben utilizar sus cuentas de correo personal para manejar información de la Entidad.

- Los funcionarios, contratistas y colaboradores de la Superintendencia no deben manipular los dispositivos de almacenamiento interno o cualquier otro componente interno de los equipos de cómputo y dispositivos que sean asignados por la Entidad. Solamente el personal de soporte técnico calificado y autorizado por la STI puede realizar estos procedimientos.
- Todo funcionario, contratista y colaborador debe registrar el ingreso y salida de elementos tecnológicos en la bitácora de ingreso (solicitados por el personal de seguridad) en las instalaciones de la Entidad.

Para el proceso de desvinculación o cambio de rol:

- La gestión de inactivación de los privilegios de acceso sobre los sistemas de información y/o herramientas de la Entidad en el caso de los funcionarios estará a cargo del jefe directo o para contratistas será el supervisor del contrato.
- Todo funcionario, contratista y colaborador que se retire de la Entidad o cambie de dependencia o rol, debe elaborar un acta de entrega dirigida al jefe de la dependencia o supervisor del contrato de cualquier activo de información mantenido, usado o producido durante su vinculación con la entidad.
- Los funcionarios, contratistas y colaboradores deben salvaguardar y proteger los activos asignados para el desempeño de sus labores u obligaciones. En el caso que dichos activos hayan sufrido algún tipo de daño debe establecerse la causa que lo originó para determinar los correctivos o eventuales sanciones a que haya lugar, según sea el caso. Estas últimas en el marco del debido proceso.

5.5. Política de gestión de activos.

La Entidad debe identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de esta. La Superintendencia Nacional de Salud establece que:

- El propietario de la información o los responsables de procesos de la Entidad deben mantener el inventario de activos actualizado anualmente identificando el responsable en su generación, administración y/o custodia a nivel de proceso. Así mismo, deben clasificar los activos con relación a los niveles de acuerdo con el tipo de información (pública, reservada o clasificada).

Lo anterior, según los siguientes lineamientos:

- La información debe ser clasificada en función de la criticidad o susceptibilidad respecto a la divulgación, pérdida o modificación no autorizada.
- Se debe etiquetar la información física o digital que genere la Entidad como información pública, reservada o clasificada. Esto aplica a los correos electrónicos e información documentada administrada por el proceso de gestión documental. Los comunicados públicos de la Entidad no requieren ser etiquetados.
- Todos los funcionarios, contratistas y colaboradores deben proteger la información almacenada en dispositivos con relación a su acceso, uso, transporte, almacenamiento y eliminación, acorde con su nivel de clasificación.
- Los dispositivos removibles asignados a los funcionarios, contratistas y

colaboradores de la Entidad deben ser devueltos en los términos y condiciones definidas al momento de la asignación.

- La STI actualizará de manera anual los activos de información de cada proceso y éstos podrán ser consultados en la página web de la SNS.

5.6. Política de control de acceso.

La Superintendencia realizará la identificación e implementación de controles que limiten el acceso a la información y a las instalaciones donde se procesa. Por lo anterior, se establece que:

El acceso a los activos de información se permite únicamente al personal autorizado ya sea con vinculación laboral o contractual vigente, en caso de usuarios internos o con acuerdo de intercambio de información entre las entidades para usuarios externos y/o proveedores. De acuerdo con los siguientes lineamientos:

- El personal que tiene privilegios de acceso a los sistemas de información debe contar con vinculación laboral o contractual vigente con la Superintendencia o con terceros que tengan contrato actual con la Entidad y autorización de acceso al activo.
- En el caso de las entidades públicas o privadas se debe formalizar el intercambio de información para el acceso a la información de la Entidad, teniendo en cuenta los lineamientos de MinTIC u otras buenas prácticas
- El acceso a los sistemas de información de los usuarios que son contratados a través de terceros (contratistas de la entidad o entidades externas) requiere diligenciar la correspondiente autorización o acuerdo de confidencialidad.
- Los usuarios de entidades externas deben contar con la autorización de su

colaborador designado1, definido en el marco del acuerdo de intercambio de información y la autorización del proceso propietario del activo.

- Se deben ejecutar los procedimientos definidos por la STI por parte de las áreas de la Entidad para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información.
- Las credenciales de acceso a los sistemas de información de la Entidad deben ser individuales y deben ser personales e intransferibles.
- El manejo indebido de las credenciales de uso es responsabilidad del usuario asignado y será a quien se le solicite las explicaciones pertinentes por el uso inadecuado.

5.7. Política de control de acceso.

Las contraseñas de los usuarios deben cumplir con los siguientes parámetros:

- Deben tener una longitud mínima de 8 caracteres alfanuméricos.
- Deben contener al menos un número, una letra minúscula, una mayúscula y un carácter especial “#$%() ¡”.
- Las contraseñas son de uso personal y por ningún motivo se debe divulgar a otros usuarios.
- Se deben cambiar una vez se notifique la creación o asignación de credenciales de acceso genéricas.
- Posteriormente deben ser cambiadas mínimo cada 45 días.
- Para la creación de los usuarios a través de sistemas de información o directorio activo, se entregará una contraseña temporal al usuario por medio

[1] Colaborador designado: Es la persona al interior de la entidad externa que articula el intercambio de información con la SNS.

de correo electrónico o llamada telefónica. Es obligatorio que el usuario deba cambiarla desde su primer uso.

- Los usuarios no deben usar las credenciales de acceso de otros usuarios, ni intentar apoderarse de sus claves, tampoco probar una cantidad de combinaciones posibles con el fin de identificar contraseñas de usuarios legítimos para acceder a un Sistema de Información o equipo de cómputo de la Entidad.
- Se deben generar registros de auditoría respecto al ingreso en los Sistemas de Información críticos de la Superintendencia Nacional de Salud.
- Se debe controlar el acceso a los registros de auditoría de sistemas de información para que solamente el personal autorizado, pueda acceder a ellos en el marco administración de la plataforma tecnológica.
- Los sistemas de información de la Superintendencia deben contar con mecanismos de identificación individual de los usuarios y procedimientos para el control de acceso a los mismos. En caso de credenciales de acceso generadas en sistemas de información, para el acceso por parte de otros sistemas (interoperabilidad o intercambio de información), estas deben ser nombradas de manera genérica, una por cada sistema de información.
- En caso de pérdida, robo, daño, alteración, divulgación no autorizada y/o fuga de información física o digital como consecuencia del descuido o actuación riesgosa por parte de un funcionario, contratista o colaborador de la Entidad, este último asumirá las sanciones a que haya lugar (disciplinarias o derivadas del contrato).
- Los usuarios no deben acceder a la información de la Entidad sin firma previa del acuerdo o compromiso de confidencialidad.

El jefe inmediato o el supervisor del contrato según sea el caso, debe informar a la

Dirección de Talento Humano o Dirección de Contratación, así como a los administradores de sistemas de información involucrados, las novedades relacionadas con el retiro o traslado del funcionario, contratista o colaborador de la Entidad.

5.8. Política de criptografía.

La SNS genera, procesa, almacena, despliega y transmite información por lo cual la Entidad establece su compromiso de gestionar lo necesario para la protección de esta principalmente aquella que ha sido categorizada como clasificada o reservada, considerando la confidencialidad, integridad, autenticidad y no repudio de la información, durante todo el ciclo de vida de esta. Para tal fin, la SNS debe:

- Realizar una evaluación de riesgos de seguridad con el fin de establecer el nivel de protección necesario, mediante la aplicación de controles criptográficos.
- Establecer controles para la gestión de las claves criptográficas.
- Se definen por defecto el uso del algoritmo criptográfico AES-256 para cifrado simétrico, ECDSA con curva NIST P-256 para cifrado asimétrico y el uso del protocolo TLS en el almacenamiento y comunicaciones cifradas de la entidad.
- Implementar una herramienta de cifrado en todos los equipos de cómputo de la Entidad, autorizada por el grupo de Seguridad Digital adscrito a la STI, para el cifrado de información institucional, que soporte esquemas de cifrados híbridos.
- Considerar las medidas de protección para el intercambio de información cifrada, usando esquemas de cifrados híbridos, o cuando se requiera del transporte o distribución, tanto manual como electrónica de las claves

criptográficas.

- Mantener copia de las claves de cifrado en un lugar físico seguro, de forma que la recuperación de la información cifrada sea posible en caso de ausencia temporal o definitiva del custodio o responsable de las claves y de la información cifrada.
- Determinar que los propietarios son los responsables del cifrado de la información que tengan a su cargo.
- Permitir la auditabilidad de todo proceso de cifrado de la información por parte de los responsables de este, incluyendo el registro (logging) de las actividades correspondientes.
- Utilizar el algoritmo de Hash SHA-256 para garantizar
- Mantener actualizada la documentación sobre la utilización de la criptografía en la Entidad incluyendo las actividades sobre la gestión de las claves para el cifrado de información.

En los casos que se requiera el almacenamiento de información de tipo confidencial, personal o sensible en servicios de nube. Ésta se debe mantener en la medida de lo posible cifrada para evitar su divulgación o accesos no autorizados.

5.9. Política de seguridad física y del entorno.

La Superintendencia propende en la definición e implementación de controles relacionados con la seguridad física en las instalaciones de la Entidad. Por consiguiente, se establece que:

La Dirección Administrativa debe implementar los controles para el acceso físico a las instalaciones de la Entidad. Lo anterior con el fin de prevenir la pérdida de activos de la Entidad, el daño o interceptación de la información almacenada en

medios físicos, bien sea en archivo o bodega de la Entidad. Para ello téngase en cuenta los siguientes lineamientos:

- No se permite comer, consumir líquidos o fumar cerca de las instalaciones para procesamiento de información o centros de cableado.
- La Dirección Administrativa debe hacer seguimiento de las condiciones requeridas de suministro eléctrico y condiciones ambientales tales como: temperatura y humedad para determinar los escenarios que puedan afectar negativamente la operación de las instalaciones de procesamiento de información o centros de cableado. Así mismo se deben realizar mantenimientos periódicos sobre los elementos de suministro eléctrico y controles ambientales.
- El cableado de energía eléctrica y datos debe estar debidamente protegido para evitar la interceptación, interferencia o daño, por medio de canaletas o bandejas definidas para tal fin. Es responsabilidad de todos los funcionarios, contratistas y colaboradores informar el incumplimiento de este numeral.
- No se permite tomar fotografías o videos dentro de las instalaciones de procesamiento de información o centros de cableado sin la autorización de la STI.
- La configuración de máquinas de copiado o multifuncionales está permitida únicamente a personal técnico autorizado por la STI.
- La Dirección Administrativa autorizará la salida de equipos y expedientes físicos de la Entidad.
- La STI debe realizar el borrado seguro de la información almacenada en discos duros (portables o de equipos de cómputo) que se entreguen al proveedor de servicios o que se reasignen a otro usuario para su uso.

- La STI debe realizar la aplicación de la guía de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario o contratistas haya sido retirado de la SNS.
- La STI realizará un inventario detallado del Hardware y del Software adquirido en la entidad.
- Los usuarios deben retirar de forma inmediata todos los documentos confidenciales que envíen a las impresoras. No se debe reutilizar papel que contenga información confidencial o privada.

Es responsabilidad de los funcionarios, contratistas y colaboradores:

- Mantener los equipos de acuerdo con las especificaciones de los fabricantes.
- Registrar las fallas y mantenimientos correctivos, como evidencia de la gestión.
- Verificar que el mantenimiento preventivo o correctivo es realizado por el personal calificado y autorizado por la STI.
- El retiro inmediato de documentos impresos de las impresoras

La STI debe programar actividades de mantenimiento periódico en los equipos de cómputo y portátiles adquiridos por la Entidad.

- El usuario debe validar el correcto funcionamiento de los equipos al finalizar el mantenimiento. Los usuarios procederán a firmar el reporte que entrega el técnico siempre y cuando el equipo se encuentre en óptimas condiciones.
- El usuario debe notificar a la STI o a la mesa de servicios tecnológicos en caso de presentar inconformidad o daño de los elementos o el servicio.

5.10. Política de gestión de contraseñas.

Es responsabilidad de los usuarios proteger la información, herramientas y sistemas

de información a su cargo para minimizar el riesgo de exposición de la información sensible y activos críticos, cumpliendo con los siguientes lineamientos:

- Configurar las credenciales de acceso en los equipos de cómputo o dispositivos de los usuarios (Usuarios y contraseñas que cumplan con los requisitos de seguridad).
- Actualizar periódicamente las contraseñas, cumpliendo las características según la política de control de acceso.
- No escribir contraseñas o información sensible en papeles o documentos a la vista.
- No desatender el equipo de cómputo o dispositivo móvil. En este sentido, debe bloquear el equipo de cómputo, cada vez que se retire de su lugar de trabajo.
- Se deben implementar controles de doble factor de autenticación para el acceso a correo electrónico y sistemas de información.
- En los equipos de cómputo suministrados por la Entidad, usar exclusivamente software autorizado por la STI. El Grupo de Infraestructura deberá parametrizar una política en el Directorio Activo, con una lista previamente definida, para cada grupo funcional de usuarios.
- Si se requiere instalar software adicional se requerirá realizar un análisis de riesgos sobre la instalación y este análisis lo realizará la Mesa de Ayuda en conjunto con el Grupo de Seguridad Digital.
- No desatender, ni dejar a la vista documentos o información sensible para la Superintendencia Nacional de Salud.
- Mantener bajo llave documentos físicos, dispositivos móviles, unidades de almacenamiento como son (USB, discos duros, discos extraíbles, CD, DVD), cuando estos no se estén usando.
- Los equipos de cómputo asignados por la Entidad deben tener configurado

solo el papel tapiz y el protector institucional de la Superintendencia Nacional de Salud.

- Los usuarios son responsables de la información que es enviada desde el computador institucional o personal, correo electrónico y/o usuarios en los diferentes sistemas de información.

5.11. Política de seguridad de las operaciones.

La Superintendencia propende en la definición de controles de seguridad relacionados con el procesamiento de la información de la Entidad. A partir de lo anterior, se establece que:

Se debe planear, probar y registrar todo cambio en la infraestructura tecnológica y sistemas de información de la Entidad. Esto para asegurar los recursos como: dotación tecnológica, infraestructura y sistemas de información indispensables en la operación.

Se deben implementar controles con el objetivo de reducir los accesos o cambios no autorizados en los ambientes donde se desarrollan los sistemas de información de la Entidad y terceros con relación contractual. Para esto se establecen los siguientes lineamientos:

- Se debe planificar y controlar los cambios relacionados con el mantenimiento o ajuste de los procedimientos, la infraestructura y los sistemas de información que se encuentran a su cargo de manera segura, garantizando la confidencialidad, disponibilidad e integridad de los activos de información.
- Los usuarios no deben realizar cambios en los equipos de cómputo de trabajo a nivel hardware y/o software relacionado con la configuración del equipo.

Estos cambios podrán ser realizados únicamente por la STI de la Entidad o por personal autorizado como administrador del equipo de cómputo.

- La STI debe proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información.
- Se debe documentar y controlar el paso a producción y la administración de los ambientes, que tengan las mismas características técnicas o similares para validar el funcionamiento de las aplicaciones.
- Todos los cambios deben ser planificados y se deben realizar por ventana de mantenimiento programada para no afectar los horarios de operación en la Entidad, salvo aquellos de carácter urgente autorizados por los directores o jefes de Oficina de la Entidad, los cuales deben ser documentados.

- Se debe restringir el acceso a los ambientes de producción. Toda excepción debe ser aprobada por la STI.
- Los equipos que manejan información de la Superintendencia deben estar protegidos con antivirus operado por la misma Entidad y su actualización automática.
- La herramienta de control de código malicioso debe realizar análisis de los equipos de cómputo.
- La STI podrá hacer seguimiento al tráfico de la red al tener evidencias de actividad inusual o degradación en el desempeño.
- La STI debe mantener documentados los incidentes de seguridad de la información que sean reportados por funcionarios, contratistas y colaboradores de la Entidad. De igual manera hacer seguimiento a los eventos inusuales que se presentan y afecten la seguridad de la información o tengan un impacto considerable para el desempeño de los sistemas informáticos.

- Se prohíbe el uso de software no autorizado por la STI, en los equipos cómputo proporcionados por la Entidad.
- La STI debe llevar a cabo revisiones regulares del software instalado en los equipos de cómputo de la Entidad.
- Se debe realizar un reporte y recuperación de la información involucrada en ataques con software malicioso.
- Los Directores y Jefes de área y/o oficinas, o sus delegados son responsables de gestionar el respaldo de toda la información correspondiente a su respectivo grupo de trabajo, almacenada en equipos de cómputo, en los servicios de almacenamiento dispuestos por la STI.
- La STI debe establecer e implementar un plan o protocolo de copias de respaldo para servidores.
- La STI debe determinar el plan o protocolo para la restauración de información de servidores.
- El Grupo de Infraestructura Tecnológica de la STI debe proporcionar o gestionar el espacio físico y digital para el almacenamiento de copias de seguridad.
- El Grupo de Infraestructura Tecnológica de la STI debe establecer el ambiente para la restauración de copias de seguridad con el propósito de certificar la calidad de esta. Las restauraciones se deberán probar de manera periódica y las pruebas y resultados deben estar documentados.
- El Grupo de Infraestructura Tecnológica de la STI debe definir roles y responsabilidades para realizar las actividades de copias de respaldo.
- La Dirección Administrativa es responsable de definir los tiempos para la retención de copias de seguridad e históricos según las tablas de retención documental. Los tiempos de retención de copias de seguridad deberán ser definidos en concordancia con las TRD y con los lineamientos de la Política

de copias de seguridad de la información (5.20).

- La STI realiza el control y seguimiento al proceso de copia de respaldo de la información y restauración.
- Se deben registrar intentos de acceso a los sistemas de información que sean exitosos y rechazados.
- La STI es responsable de hacer cambios en la configuración del sistema y uso de privilegios.
- La STI es responsable de realizar el monitoreo de las aplicaciones y programas utilitarios del sistema.
- La STI debe tener un inventario sobre direccionamiento y protocolos de red.
- Se debe asegurar que la información de los registros o logs sean protegidos contra toda alteración y acceso no autorizado.
- Los administradores técnicos de sistemas de información deben gestionar las vulnerabilidades técnicas y deben realizar la adopción de medidas para el control del riesgo.
- Los administradores técnicos de sistemas de información deben realizar la implementación de controles de seguridad aplicables a sistemas de información para mitigar el riesgo de interrupción en los procesos de la Entidad.
- La STI debe brindar lineamientos a los Administradores Funcionales de las herramientas de la Superintendencia, para unificar los criterios y manejar una única política interna de administración de usuarios dentro de la Entidad.
- La STI debe establecer estrategias de seguridad que permitan tomar acciones ante las vulnerabilidades que puedan afectar la información.
- La STI debe detectar, reportar, valorar y gestionar las vulnerabilidades técnicas de los activos de información, a fin de evitar el compromiso de la confidencialidad, disponibilidad e integridad de la información en la Entidad.

- La STI debe definir e implementar planes de remediación para la solución de las vulnerabilidades de acuerdo con las estrategias que se definan así mismo se debe hacer seguimiento a los planes de remediación y medidas de control correspondientes de las vulnerabilidades reportadas enfocados en la mitigación de los riesgos asociados a las mismas.
- La STI debe gestionar lo necesario para que los proveedores de infraestructura tecnológica certifiquen que los equipos y servicios de TI suministrados y prestados a la SNS se encuentran libres de códigos maliciosos y vulnerabilidades técnicas, realizando los monitoreos y análisis periódicos necesarios para ello.
- La STI debe realizar anualmente, como mínimo, una (1) prueba de hacking ético a la infraestructura y sistemas de información de la SNS, por parte de personal competente y calificado. Los resultados de estas pruebas deben ser consideradas dentro de la planeación de remediación, en coherencia con la criticidad y nivel de exposición de las vulnerabilidades encontradas.

Los lineamientos específicos relacionados con la planificación, ejecución, almacenamiento, retención y restauración de copias de seguridad de la información se regirán por la **Política de copias de seguridad de la información (numeral 5.20)**, por el Manual para las copias de seguridad de la información, los cuales hacen parte integral del Sistema de Gestión de Seguridad y Privacidad de la Información de la Entidad.

5.12. Política de seguridad de las comunicaciones.

Esta política consiste en la definición e implementación de controles relacionados con el aseguramiento de las redes de comunicaciones y/o servicios de la Entidad.

Por consiguiente, se establece que:

- La STI debe restringir la conexión de los dispositivos a través del puerto USB, Bluetooth o cualquier otra tecnología inalámbrica.
- La STI debe restringir los privilegios de administrador a nivel de sistema operativo. (Para equipos asignados por la STI o por cualquier operador).
- Sólo se permite el uso de software licenciado e instalado por personal autorizado a través de la STI para equipos asignados por la STI.
- Los funcionarios, contratistas y colaboradores deben cumplir las políticas, procedimientos y controles para la transferencia de información establecidos por la STI.
- Implementar los lineamientos establecidos por Superintendencia y la STI para la transferencia segura de información entre la entidad y las entidades externas.
- Proteger adecuadamente la información incluida en la mensajería electrónica.
- La STI debe implementar las medidas de detección y protección contra el código malicioso que pudiere ser transmitido a través de las comunicaciones electrónicas.
- La STI debe controlar el uso de la conectividad inalámbrica.
- No se permite el acceso a páginas de pornografía, drogas, alcohol, música, concursos en la web, juegos, violencia u otras, que no tengan relación con el desempeño de funciones o actividades propias de la Superintendencia Nacional de Salud.
- No se permite descargar, usar, intercambiar y/o instalar (juegos, música, videos, películas, imágenes, protectores, fondos de pantalla, software, información y/o productos) que atenten contra la propiedad intelectual de sus

autores o que también contengan (archivos ejecutables, herramientas de hacking y software malicioso) capaces de generar un riesgo de información para la entidad.

- La entidad puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación de cada usuario desde cualquier puerto y/o protocolo utilizado. Esto como parte de las funciones de administración de la plataforma tecnológica.
- Los usuarios serán responsables del uso adecuado tanto del internet como de la mensajería interna. En ningún momento aquellos podrán ser utilizados para prácticas ilícitas que atenten contra la entidad, terceros, legislación vigente, políticas o lineamientos de seguridad y privacidad de la información.
- Los funcionarios, contratistas y colaboradores no podrán asumir en nombre de la entidad posiciones frente a encuestas de opinión, foros, redes sociales u otros medios similares.
- Los funcionarios, contratistas o colaboradores que hagan parte de redes sociales virtuales como Facebook, Twitter, LinkedIn, Instagram u otros que permitan cualquier tipo de opinión no deberán publicar datos relacionados con la Superintendencia.
- La mensajería instantánea y el correo electrónico de uso interno o externo deben ser usados exclusivamente en el desempeño de funciones y operatividad de la entidad.

La información, los mensajes y correos electrónicos son propiedad de la Superintendencia, que está facultada para inspeccionar, registrar y evaluar información intercambiada por estos medios según las funciones de administración de la plataforma tecnológica.

De acuerdo con el numeral anterior, a continuación, se relacionan los siguientes ítems:

- Solo se permite el uso de las herramientas colaborativas autorizadas por la STI, para mensajería instantánea interna y externa con actividades propias de la Superintendencia.
- Se prohíbe el uso de cuentas de correo externas (Outlook personal, Gmail, Yahoo, entre otros) o servicios de nube no proporcionados por la STI, en la red de la entidad.
- No se permite enviar o reenviar cadenas de correo, mensajes con contenidos de carácter corporativo, religioso, político, racista, sexista, pornográfico, publicitario no corporativo u otro tipo que atenten contra la dignidad de las personas, afecten los sistemas internos y de terceros. Tampoco es viable el envío de aquellos que estén en contravía de las leyes, la moral, las buenas costumbres, incitando a prácticas ilícitas o promoviendo a actividades ilegales.
- La información sensible de la entidad que requiera ser enviada fuera de sus instalaciones debe seguir los procedimientos de articulación interinstitucional.
- Ningún funcionario, contratista o colaborador no autorizado por la STI podrá revisar correos electrónicos institucionales de los usuarios o sus correspondientes registros de auditoría. Ello, sin perjuicio de los requerimientos legales y administración de la plataforma tecnológica que se pueda presentar.
- Los usuarios deben evitar el envío de correos electrónicos con información considerada como clasificada o reservada a terceros y/o personal interno.
- Los funcionarios, contratistas y colaboradores son responsables de la información que se envía desde su correo electrónico institucional.

- La STI debe asignar las medidas, restricciones y controles asociados al reenvió de información sobre medios de comunicación (por ejemplo, el reenvió automático del correo electrónico hacia direcciones externas).
- La STI debe realizar la socialización de directrices, políticas y/o buenas prácticas relacionadas con el intercambio de información.
- La STI debe definir estándares técnicos mínimos para la transmisión de la información con entidades externas y procesos de la Entidad.
- La STI define los requisitos de seguridad en la plataforma de correo electrónico para transferencia de información.
- La STI debe establecer la propiedad y responsabilidad para la protección de datos, derechos de copia conforme con las licencias de software y consideradas similares.
- La STI y el supervisor del contrato con el proveedor deben socializar, sensibilizar y divulgar las campañas para el buen uso de los sistemas de mensajería electrónica.
- La STI es responsable de identificar, revisar, documentar y actualizar periódicamente los requisitos para los acuerdos de confidencialidad.

5.13. Política de adquisición, desarrollo y mantenimiento de sistemas.

Esta política consiste en la implementación de controles en el marco del ciclo de vida del desarrollo de software en la Entidad, liderada por la STI en articulación con los responsables técnicos de sistemas de información de la entidad. Así las cosas, en la Superintendencia se debe realizar la adquisición o desarrollo de software, para su posterior despliegue en ambiente productivo, acorde a los siguientes lineamientos:

- Se debe establecer el plan de trabajo con actividades, responsables, tiempos

y fechas de ejecución de los proyectos relacionados con la adquisición, el desarrollo y mantenimiento de software, bajo la metodología y procedimiento vigente en la Entidad.

- Se debe realizar el levantamiento de las especificaciones funcionales y no funcionales, así como el diseño con mínimo de historial de usuarios y criterios de aceptación, en el marco del procedimiento vigente.
- Los responsables técnicos de los sistemas de información deben gestionar la documentación y actualización de la arquitectura de los sistemas de información que hacen parte de la entidad, en el marco del procedimiento vigente.
- Los responsables técnicos de sistemas de información deben implementar escenarios de pruebas para garantizar que la solución tecnológica cumpla con los requisitos y necesidades de seguridad, siguiendo los lineamientos de la STI.
- Se debe ejecutar pruebas unitarias e integrales de la funcionalidad creada o modificada.
- Se debe incorporar los requerimientos de seguridad de la información en la documentación para nuevos desarrollos o nuevas funcionalidades de los sistemas de información.
- Se debe incorporar los requerimientos de seguridad de la información en los sistemas de información que son operados en la actualidad bajo la administración de la entidad.
- Se debe realizar el análisis, identificación y el correspondiente tratamiento de los riesgos en la fase de diseño a fin de establecer los controles de seguridad adecuados.
- Se debe realizar revisiones, previo al paso a producción, sobre lógica del código fuente de la aplicación para reducir la probabilidad de errores de

seguridad en la codificación.

- Se debe gestionar el Hacking ético periódicamente en las herramientas de producción y/o ambientes controlados, bajo los lineamientos de la STI.

- Todo desarrollo de sistemas de información realizado en la entidad o a través de terceros debe ser verificado en ambiente de pruebas. Adicionalmente debe ser validado y avalado por el usuario final.
- Se debe implementar el control de las versiones de componentes e ítems de configuración de las aplicaciones, a través de la herramienta provista por STI para el desarrollo de software.
- Todo cambio en los sistemas de información debe contar con aprobación del propietario o responsable funcional de la información.
- Se debe implementar controles de autenticación para garantizar que el usuario se identifique y en esa medida solo quienes estén autorizados accedan a sistemas de Información.
- Se debe garantizar que las contraseñas se protejan contra modificación, destrucción, copia o divulgación no autorizada mediante almacenamiento cifrado en las bases de datos.
- Se debe implementar controles que determinen el nivel de accesos a la información, menús, parametrización del sistema y demás componentes para que administren los sistemas de información.
- Todos los sistemas de información deben contar con logs (registros de auditoría) que detallen las actividades que se realizan en el sistema. De igual manera se deben implementar registros de auditoría para detección de anomalías e indicadores claves de éxito (PKI).
- Se debe almacenar el histórico correspondiente a los datos gestionados mediante los sistemas de información de la entidad.

- Se debe implementar controles en la administración de las fallas en los sistemas de información de la entidad, generando excepciones controladas cuando se genere un error, evento o incidente.
- Se debe implementar controles que aseguren el funcionamiento de sistemas de información y software en uso, cuando se realicen actualizaciones o cambios a nivel de sistemas operativos o configuración.
- Se debe realizar validaciones para asegurar la calidad de los datos que son ingresados en sistemas de información evitando ataques de inyección de código.
- La STI debe implementar mecanismos de cifrado y control de acceso a la información que sean visibles a los usuarios autorizados.
- La STI debe implementar los protocolos seguros (SSL) de cifrado y control de fuga de información.
- La STI debe adquirir certificados de sitio seguro para ambientes de producción expuestos en la red pública que aseguren la transmisión de información.
- La STI debe asegurar los canales de comunicación para minimizar el riesgo de fuga de información.
- Se debe tener un registro de las configuraciones y funcionalidades de los sistemas de información que sirva de consulta para la revisión errores del sistema, capacitaciones y transferencias de conocimiento relacionadas con el mismo.
- Se debe usar técnicas de validación de identidad en directorio activo y en sistemas de información de la Entidad.
- Se debe definir roles y perfiles de usuario para establecer los niveles de acceso asociados a la configuración técnica de los sistemas de información.
- La STI debe implementar controles para la modificación del código fuente.

- Todos los códigos fuentes deben estar registrados y controlados por la STI, bajo la herramienta de control de versiones definida para tal fin. Será responsabilidad de los administradores técnicos de desarrollo realizar el registro, actualización, o cambio en los códigos fuentes de cada una de las aplicaciones.
- Se debe controlar el número de sesiones por usuario para evitar el uso de credenciales de acceso compartidas.
- Se debe dimensionar la capacidad requerida de la infraestructura que soporte la publicación de sistemas de información en ambiente productivo.
- Se debe controlar el acceso a los ambientes de preproducción y herramientas para el manejo del código fuente.

5.14. Política de relaciones con los proveedores.

Esta política consiste en implementación de controles relacionados con el aseguramiento de los productos o servicios suministrados por terceros, que soportan la operación de la entidad. Se deben gestionar los riesgos de seguridad de la información asociados con la cadena de suministro, que afecten la continuidad de la operación o servicios de tecnología y comunicación, teniendo en cuenta los siguientes lineamientos:

- La STI debe establecer los requisitos de seguridad de la información necesarios para mitigar los riesgos de seguridad de la información asociados con la cadena de suministro que impacten la continuidad de la operación o los servicios de tecnologías y comunicación.
- La STI debe llevar a cabo las auditorías de los proveedores y la revisión de reportes respecto a auditorias independientes, además del seguimiento a los hallazgos identificados.

- La STI debe gestionar los incidentes de seguridad con proveedores, en el marco de los acuerdos definidos.
- La STI debe revisar los aspectos de seguridad de la información de las relaciones de los proveedores con sus terceros.
- La STI debe asegurar que el proveedor mantenga una capacidad de servicio suficiente junto con planes ejecutables, para asegurar el mantenimiento de niveles de continuidad del servicio acordados después de fallas considerables en el mismo o luego de un desastre.
- La STI debe establecer acuerdos de niveles de servicio con proveedores y entregar informes de seguimiento al cumplimiento.
- Los proveedores deben reportar a los supervisores, el listado de personal que se ha desvinculado de su compañía para retirar los accesos a servicios y/o información propia de la entidad.
- Los proveedores de servicios tecnológicos deben garantizar que toda política de seguridad implementada por aquellos cumpla con las políticas y controles de seguridad de la información de la Entidad.
- Todos los procesos y/o dependencias de la Superintendencia Nacional de Salud, que necesiten realizar adquisiciones y/o contrataciones de herramientas y/o servicios tecnológicos incluyendo, pero sin limitarse a sistemas de información, componentes tecnológicos etc., deberán contar con concepto de viabilidad técnica por parte de la STI, incluyendo seguridad de la información.
- Así mismo, en los casos en los que se requiera adquirir y/o contratar servicios de tratamiento y/o protección de activos de información y tecnológicos, entre otros, pero sin limitarse al almacenamiento de la información física y/o digital, infraestructura etc., debe asegurar que el proveedor cuente con los mecanismos y/o controles de seguridad adecuados para la prestación del

servicio contratado.

- El supervisor de contrato debe asegurar que el proveedor y/o tercero conoce la ***Política de Gestión de Incidentes de Seguridad de la Información*** junto con los respectivos canales de comunicación establecidos por la Superintendencia Nacional de Salud ante la materialización de incidentes de seguridad.
- Todos los proveedores y/o terceros que necesiten y/o requieran realizar modificaciones y/o instalaciones de activos los activos de información y/o tecnológicos, entre otros, pero sin limitarse a sistemas de información, servidores etc., deben cumplir con todos los lineamientos establecidos por la Superintendencia Nacional de Salud a través de las Políticas internas y de seguridad de la Información de la entidad. En este sentido, la STI es la responsable de verificar y/o validar el cumplimiento de estos, así como el emitir y/o reportar las recomendaciones y/o vulnerabilidades al respectivo proveedor del servicio previa solicitud del proceso dueño del producto y/o servicio del prestado por el proveedor.

- Así mismo, todas las acciones que impliquen modificaciones, mantenimientos, revisión de los servicios de la infraestructura tecnológica, comunicaciones o equipos de suministro de la entidad junto con las respectivas instalaciones a las que haya lugar, se debe realizar siguiendo lo establecido en la ***Política de Seguridad de Gestión de Cambios.***
- Todos los proveedores y/o terceros pueden conectarse de manera remota única y exclusivamente por los mecanismos y/o herramientas definidas por la Superintendencia Nacional de Salud a través de la STI, entre otras por Virtual Private Network (VPN), cuando esto así se considere necesario para el cumplimiento de las obligaciones contractuales a las que haya lugar. En caso contrario, se debe solicitar la debida autorización de manera formal a la

STI, incluyendo Seguridad de la Información quienes analizarán, revisarán y/o validarán la justificación de dichos requerimientos, los cuales pueden aprobarlo o denegarlo.

- Permisos y/o accesos deben ser solicitados por el líder del proceso y/o supervisor de contrato ante la STI, incluyendo al Grupo de Seguridad de la Información, en donde dichos permisos y/o accesos se pueden otorgar con la finalidad de brindar soporte a dispositivos tecnológicos o sistemas de información, revisar errores de funcionamiento o prestar servicios de monitoreo y/o seguridad. En este sentido, la Superintendencia Nacional de Salud, a través de la STI, debe implementar controles que contribuyan con la limitación de acceso sobre estos junto con el registrar las acciones ejecutadas para seguimiento y aunado a la supervisión visualmente del trabajo realizado por medio de acompañamiento permanente.
- Todos los proveedores y/o terceros deben a utilizar única y exclusivamente software legal en cumplimiento de lo establecido en la Ley 603 de 2000 o las normas que la reemplacen, modifiquen o adicionen. En este sentido, el proveedor y/o tercero asume toda la responsabilidad, legal, civil, penal y/o la que haya lugar en caso de incumplimiento de la citada ley.
- Todos los proveedore y/o terceros que presten servicios de desarrollo de software para la Superintendencia Nacional de Salud, debe utilizar las mejores y/o buenas prácticas en la materia, asegurando el desarrollo seguro de las aplicaciones y/o sistemas de información.
- Todos los proveedores y/o terceros que presten servicios de desarrollo de software para la Superintendencia Nacional de Salud, debe garantizar que previo a la publicación de aplicaciones y/o sistemas de información en ambientes de producción y/o entrega de funcionamiento hacia la Superintendencia Nacional de Salud, realizó la respectiva revisión de códigos

fuentes estático y dinámico que permitan las identificaciones de las vulnerabilidades existentes sobre estos junto con las correspondientes subsanaciones a las que haya lugar, por medio de la presentación de un informe que refleje lo mencionado, el cual debe tener la aprobación de la STI incluyendo seguridad de la información. En este sentido, la no ejecución de este tipo de revisiones no exime al proveedor de su respectiva responsabilidad.

- Todos los proveedores y/o terceros que tengan acceso a la información propiedad de la Superintendencia Nacional de Salud, deben establecer un procedimiento de borrado seguro que garantice la adecuada eliminación propiedad de la entidad. En este sentido, dicho procedimiento debe ser desarrollado y socializado a la STI incluyendo seguridad de la información antes del inicio de la relación contractual.
- Así mismo, todos los proveedores y/o terceros deben asegurar que el personal a contratar por parte de este para la ejecución de actividades para la Superintendencia Nacional de Salud cuenta con las capacidades profesionales o técnicas requeridas para la relación contractual con la entidad, adicionalmente, esta selección de personal debe realizar la respectiva verificación de la hoja de vida, incluyendo la revisión y validación de referencias incluyendo antecedentes sumado a las revisiones dispuestas por el proveedor.
- Todos los proveedores y/o terceros que presten servicios y/o herramientas tecnológicas a la Superintendencia Nacional de Salud, debe garantizar que las diferentes herramientas y/o servicios tecnológicos cuentan con las diversas actualizaciones de seguridad correspondientes junto con los respectivos planes de remediación en caso de evidenciar vulnerabilidades sobre estos, así mismo, para la respectiva gestión y/o aplicación se debe

seguir lo establecido en la ***Política de Seguridad Actualizaciones de Seguridad*** y ***Política de Seguridad de Gestión de Cambios.***

- Así las cosas, la Superintendencia Nacional de Salud prohíbe expresamente cualquier actividad y/o acción que vaya en contravía de los lineamientos dispuestos en la Políticas de Seguridad de la Información de la entidad, entre otros, pero sin limitarse los siguientes:
  - Utilización de los recursos físicos y/o lógicos de la Superintendencia Nacional de Salud para actividades diferentes al cumplimiento de las obligaciones contractuales.
  - Utilización y/o conexión de dispositivos y/o equipos en la red institucional de la Superintendencia Nacional de Salud, entre otros, pero sin limitarse los siguientes: (dispositivos personales, USB, discos duros externos, etc.) junto con las diferentes aplicaciones no autorizadas por la STI.
  - Evasión de controles de seguridad implementados por la Superintendencia Nacional de Salud.

5.15. Política de gestión de incidentes de seguridad de la información.

Esta política consiste en la definición de directrices y responsabilidades para garantizar la adecuada gestión de incidentes de seguridad en la entidad. Por lo anterior se establece que:

- Los usuarios deben reportar eventos y debilidades de seguridad que involucren pérdida, divulgación o modificación no autorizada de información, por medio de la mesa de servicios tecnológicos y canales autorizados tales como el correo electrónico: soporte.oti@supersalud.gov.co.

- La STI debe determinar si el evento se considera como incidente de seguridad de la información, según las categorías y criterios de clasificación definidos en los documentos del alcance de procedimiento.
- La STI debe atender y clasificar los eventos de seguridad de la información para evaluar y determinar si se ha generado un incidente de seguridad.
- La STI debe gestionar los incidentes de seguridad de la información, determinar las lecciones aprendidas y realizar la comunicación a través de los canales adecuados.
- La STI debe recolectar la evidencia del incidente y realizar la investigación correspondiente con el fin de determinar las acciones correctivas y preventivas necesarias para mejorar el proceso.
- La STI debe conformar un equipo responsable de la gestión de incidentes de seguridad digital, con la finalidad de asegurar una respuesta eficaz durante el tratamiento de incidentes de seguridad digital.
- La STI debe definir las situaciones que deben ser catalogadas como incidentes de seguridad digital.
- La STI una vez identificado el incidente de seguridad digital, debe categorizar el respectivo incidente conforme a lo evidenciado junto con el establecimiento de la gravedad y prioridad para su tratamiento.
- La STI debe desarrollar actividades y/o procedimientos que faciliten la resolución de los incidentes de seguridad digital identificados, teniendo en cuenta aquellos incidentes de seguridad digital más habituales que se puedan materializar sobre la Superintendencia Nacional de Salud, en función de misionalidad.
- La STI debe registrar de manera detallada los diferentes incidentes de seguridad digital materializados al interior de la Superintendencia Nacional de Salud y éstos a su vez deben ser notificados y reportados al COLCERT y

a la Superintendencia de Industria y Comercio en caso de que el incidente haya afectado datos personales.

5.16. Política de gestión de la continuidad de negocio.

Esta política consiste en la identificación de planes de contingencia y continuidad para actividades y servicios críticos relacionados con la operación. Por consiguiente, se establece que:

- La STI en articulación con los procesos estratégicos, misionales y de apoyo debe identificar el grado de criticidad de las actividades y servicios de los procesos que puedan afectar la continuidad de negocio (Análisis de Impacto de Negocio).
- La STI en articulación con los procesos estratégicos, misionales y de apoyo debe establecer el plan de contingencia o continuidad del negocio, que cumpla con políticas y controles de seguridad de la Información

La Superintendencia debe identificar los recursos para la obtención de una respuesta efectiva por parte de funcionarios, contratistas y colaboradores en caso de presentarse contingencia o eventos catastróficos que afecten la operación de la entidad.

- Se debe definir un protocolo de comunicación acorde con las diferentes partes interesadas involucradas.
- La STI debe analizar, definir y establecer los requerimientos de redundancia y alta disponibilidad para sistemas de información críticos identificados, acorde al análisis de impacto de negocio. Esto también aplica para los diferentes equipos de desarrollo de la entidad.
- La STI debe evaluar y probar soluciones de redundancia tecnológica implementada para validar los planes de contingencia o continuidad.

- La STI debe definir el mecanismo y/o estrategia que cumpla con los requerimientos de alta disponibilidad a nivel de centro de datos, canales de conectividad y sistemas de información.
- La STI debe administrar soluciones de redundancia tecnológica y realizar informes sobre dichas soluciones asegurando el cumplimiento de requerimientos de disponibilidad en la entidad.

La STI debe realizar los simulacros de continuidad de negocio y contingencia tecnológica definidos para determinar el grado de eficacia y viabilidad del plan, así como hacer revisiones periódicas, para verificar que los controles establecidos sean eficaces en situaciones adversas.

Los esquemas de respaldo y restauración necesarios para la continuidad de los servicios se implementarán de conformidad con la Política de copias de seguridad de la información y los documentos técnicos asociados (DIMN14 y “Procedimiento Copias de Seguridad SI v2”).

5.17. Política de Cumplimiento.

Esta política consiste en la identificación de los requisitos legales, regulatorios, estatutarios o contractuales para el uso adecuado de los activos de información. Se establece que:

- La STI deberá gestionar el cumplimiento de la legislación correspondiente a seguridad de la información respecto a derechos de autor y propiedad intelectual.
- Todo software que sea desarrollado y usado en la entidad debe cumplir con los requerimientos legales y de licenciamiento aplicables.

- La STI será responsable de mantener el control de todas las licencias de software, hardware y aplicaciones utilizadas por la entidad.
- Se prohíbe el uso de software ilegal o no licenciado en la Entidad.
- La STI deberá realizar revisiones periódicas a los sistemas de información y estaciones de trabajo.
- Los funcionarios, contratistas y colaboradores no deben hacer distribución o modificación de software o contener archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la información.
- Cuando el personal de la Mesa de Servicios TI de la STI encuentre programas instalados en equipos de cómputo asignados a los usuarios sin el respectivo licenciamiento o autorización, deben desinstalar e informar al Grupo de seguridad y privacidad de la información.
- Todo software, páginas web, documentos, material de contenido gráfico, logos, entre otros que contengan la imagen o el nombre de la Superintendencia son propiedad de esta, bien sean creados por funcionarios, contratistas y/o colaboradores, en el cumplimiento de sus labores o para el cumplimiento de actividades contractuales propias del contrato según las formalidades del artículo 183 de la ley 23 de 1982 modificado por el art 30 de la ley 1450 de 2011.
- Se autoriza el uso de software libre aprobado por la STI. En caso de requerir un software libre sin instalación previa, se debe hacer una solicitud dirigida a la STI. Esta última llevará un inventario del software de la entidad. La solicitud debe ser realizada a través del correo soporte.oti@supersalud.gov.co.
- Los sistemas de información adquiridos o desarrollados por terceros deberán contar con un acuerdo de licenciamiento que deberá especificar las condiciones de uso del software y los derechos de propiedad intelectual del

mismo.

- Cuando adquiere un software con un subcontratista, la STI deberá revisar las condiciones contractuales para conocer el alcance, entrega de documentación de arquitectura del sistema de información, del servicio (mantenimiento y soporte), derechos patrimoniales y autorización a modificaciones futuras.
- Los sistemas de información adquiridos o desarrollados por terceros tienen que contar con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual del mismo.
- Cualquier software heredado deberá tener la licencia o soporte de transferencia del licenciamiento a la entidad. En dicha licencia, se deberá indicar si el código transferido a la entidad es objeto de modificaciones.
- Para los desarrollos propios de la Superintendencia se deberá verificar la documentación entregada, artefactos de software y las versiones correspondientes con el fin de ser preservadas en varios medios. Además, deberá guardarse una copia de respaldo externa la cual deberá registrarse ante la Dirección General de Derechos de Autor.
- Los funcionarios, contratistas y/o colaboradores responsables de publicar la información en los sitios WEB oficiales de la entidad, deberán atender el cumplimiento de las normas en materia de propiedad intelectual, referente a los derechos de autor y conexos.
- La entidad se reserva el derecho a efectuar revisiones del software instalado en equipos de cómputo suministrados por la entidad, en cuanto al licenciamiento requerido.
- La Superintendencia Nacional de Salud establecerá el cumplimiento de las disposiciones legales vigentes en Colombia sobre protección de datos

personales, incluidas la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normativas relacionadas, asegurando que todas las actividades de tratamiento se realicen conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad. El cumplimiento de esta ley se realizará a través del Programa Integral de Protección de Datos Personales aprobado por la SNS.

- La STI debe realizar revisiones y auditorías de seguridad a sistemas de información y/o al sistema de gestión de seguridad de la información. Así mismo, debe realizar inspecciones periódicas sobre temas relacionados con seguridad de la información.

5.18. Política de Seguridad BYOD (Bring Your Own Device).

La presente política de seguridad tiene como finalidad establecer los lineamientos y requerimientos mínimos necesarios que deben cumplir los dispositivos personales que sean autorizados para el uso de los recursos institucionales, entre otros los siguientes:

Todos los dispositivos personales que deseen utilizar los recursos institucionales de la Superintendencia Nacional de Salud deben cumplir como mínimo los siguientes requerimientos:

- La Superintendencia Nacional de Salud, solo aceptará los dispositivos tipo portátil y/o tabletas.[2]

[2] Se recomienda que la antigüedad de estos dispositivos no sea superior a cuatro (4) años, con la finalidad de garantizar la compatibilidad de estos con los dispositivos de la entidad.

- La Superintendencia Nacional de Salud, solo aceptará dispositivos que no hayan sido rooteados[3] o que cuenten con Jailbreak[4], su uso se encuentra totalmente prohibido en los recursos institucionales de la Superintendencia Nacional de Salud.
- La Superintendencia Nacional de Salud, solo aceptará los dispositivos con sistemas operativos que cuenten con soporte de fabricante.
- La Superintendencia Nacional de Salud, solo aceptará los dispositivos que cuenten con aplicaciones instaladas con soporte de fabricante.
- La Superintendencia Nacional de Salud, solo aceptará dispositivos que cuenten con ambientes separados para la ejecución de las actividades laborales y/o contractuales y para el manejo de la información institucional de la Superintendencia Nacional de Salud.
- La Superintendencia Nacional de Salud, solo aceptará los dispositivos que cuenten con la habilitación de solicitud de credenciales locales al instalar aplicaciones y/o al realizarse modificaciones de configuración y/o cambios en el dispositivo.
- La Superintendencia Nacional de Salud, solo aceptará los dispositivos que cuenten con la habilitación del bloqueo por inactividad, el cual debe ser menor o igual a 5 minutos, para bloquear la respectiva sesión.
- La Superintendencia Nacional de Salud, establece que el no cumplimiento de los numerales mencionados anteriormente, impedirá que se otorguen la

[3] Proceso con el que se consigue acceso 'root' al dispositivo, es decir, obtener permisos de 'superusuario' o administrador para acceder al sistema sin ningún tipo de restricción. (https://www.incibe.es/aprendeciberseguridad/jailbreaking-rooting).

[4] Proceso con el que se eliminan las limitaciones impuestas por Apple en un dispositivo con iOS. Una vez 'liberado' se podrá, por ejemplo, instalar aplicaciones de terceros que no estén en la AppStore. (Ibidem).

debida autorización para el acceso a los recursos y/o redes institucionales de la Superintendencia Nacional de Salud.

- La Superintendencia Nacional de Salud, implementará las medidas y estrategias de seguridad informática necesarias, que contribuyan a asegurar el acceso de los dispositivos personales por parte del personal previamente autorizado.
- Toda solicitud y requerimiento debe realizarse a través del Jefe de área, Líder de Proceso y/o Supervisor de Contrato o quien haga de sus veces por medio de la Mesa de Servicios e la Superintendencia Nacional de Salud.
- Todos los dispositivos que requieran acceder a los recursos y/o redes institucionales de la Superintendencia Nacional de Salud, por parte de personal externo debe ser autorizado por personal interno, quien asume la responsabilidad por las diferentes acciones que este pueda ocasionar, en caso contrario se deberá conectar a la Red de Invitados dispuesta por la Superintendencia Nacional de Salud.
- Todo el personal que acepte el acceso al uso de los recursos y/o redes institucionales de la Superintendencia Nacional de Salud, autoriza al proceso Gobierno y Gestión de Datos e Información a través de la Subdirección Tecnologías de la Información a realizar de manera aleatoria cuando revisiones del cumplimiento de los requerimientos mínimos establecidos en las Políticas de Seguridad de la Información definidos por la Superintendencia Nacional de Salud, cuando así se considere necesario.
- Todo el personal que acepte el acceso al uso de los recursos y/o redes institucionales de la Superintendencia Nacional de Salud, a través de los dispositivos personales deben demostrar que todos los aplicativos instalados en su dispositivo personal corresponden a software legal y/o legítimo y que no van en contravía de la propiedad intelectual.

- Todo el personal que acepte el acceso al uso de los recursos y/o redes institucionales de la Superintendencia Nacional de Salud, son conscientes y responsables sobre la gravedad de la utilización de software ilegítimo (crackeado), es decir, que la utilización de este tipo de software acarrea consecuencias de tipo civil y/o penal según sea el caso.
- Todo el personal que acepte el acceso al uso de los recursos y/o redes institucionales de la Superintendencia Nacional de Salud, a través de los dispositivos personales, no deben guardar las credenciales de acceso en los diferentes servicios tecnológicos de la Superintendencia Nacional de Saludo en navegadores instalados en los dispositivos.
- Todo el personal que acepte el acceso al uso de los recursos y/o redes institucionales de la Superintendencia Nacional de Salud, a través de los dispositivos personales, debe cumplir con el mínimo de características para permitir su acceso y operación, en caso de no cumplirse y/o las condiciones de estos cambien, se deshabilitará su respectivo funcionamiento y/o no se permitirá su acceso, conforme a los lineamientos definidos por la entidad.
- Todo el personal que acepte el acceso al uso de los recursos y/o redes institucionales de la Superintendencia Nacional de Salud, a través de los dispositivos personales, deben asegurar e instalar las actualizaciones correspondientes a las diferentes aplicaciones instaladas, componentes físicos y lógicos y/o sistemas operativos, es decir, instalar las actualizaciones que le apliquen.
- EL proceso Gobierno y Gestión de Datos e Información a través de la Subdirección Tecnologías de la Información, debe socializar la Política de Gestión de Incidentes de Seguridad Digital de la Superintendencia Nacional de Salud a todo el personal con acceso a los recursos y/o redes institucionales de la entidad, informando los canales oficiales de

comunicación

- Se prohíbe expresamente cualquier tipo de actividad realizada desde dispositivos personales que vaya en contravía de las Políticas de Seguridad de la Información definidas por la Superintendencia Nacional de Salud.
- Cualquier excepción a la presente política de seguridad, debe ser tramitada y aprobada por medio escrito y por adelantado por el directivo responsable de la dependencia y/o proceso, quien asume la total responsabilidad de las acciones que se puedan acarrear.
- Todo el personal que acepte el acceso al uso de los recursos y/o redes institucionales de la Superintendencia Nacional de Salud, se compromete a usar adecuadamente los diferentes recursos a los que tiene acceso, así mismo en caso de identificarse la ejecución de acciones indebidas sobre estos, estará sujeto a las medidas disciplinarias y/o contractuales correspondientes a las que haya lugar y/o las que estas deriven.

5.19. Política Actualizaciones de Seguridad.

La presente política de seguridad tiene como finalidad establecer los lineamientos mínimos necesarios que deben cumplir los responsables de los diferentes recursos físicos y/o lógicos, internos y/o externos susceptibles de actualizaciones de seguridad al interior de la Superintendencia Nacional de Salud, entre otros los siguientes:

- Los responsables de los recursos físicos y/o lógicos susceptibles de actualizaciones de seguridad, deben aplicar las diferentes correcciones críticas al momento de publicarse.
- Todas las actualizaciones de seguridad sobre los diferentes recursos físicos y/ lógicos, que no representen un riesgo para los servicios ofrecidos por la

Superintendencia Nacional de Salud, se deben realizar como máximo de manera acumulativa mensualmente.

- Los responsables de los recursos físicos y/o lógicos susceptibles de actualizaciones de seguridad, deben revisar las características y requisitos de las actualizaciones de seguridad antes de instalarlas.
- Así mismo, los responsables de los recursos físicos y/o lógicos susceptibles de actualizaciones de seguridad, deben revisar las características y requisitos mínimas necesarias que son exigidas para la aplicación de las actualizaciones de seguridad antes de instalarlas.
- Adicionalmente, los responsables de los recursos físico y/o lógicos susceptibles de actualizaciones de seguridad, deben analizar, verificar y/o revisar la aplicación de las respectivas actualizaciones de seguridad en ambiente de pruebas, reduciendo la posibilidad de errores y/o inconvenientes en ambiente de producción.
- Los responsables de los recursos físicos y/o lógicos susceptibles de actualizaciones de seguridad, deben contar con mecanismos y procedimientos que permitan deshacer los cambios realizados por las actualizaciones instaladas por estos, en los casos que se presenten inconvenientes por la aplicación de las actualizaciones de seguridad.
- Así mismo, los responsables de los recursos físicos y/o lógicos susceptibles de actualizaciones de seguridad, deben documentar todos los errores identificados productos de la instalación de las actualizaciones de seguridad.
- Adicionalmente, los responsables de los recursos físicos y/o lógicos susceptibles de actualizaciones de seguridad, deben llevar un registro de cada una de las actualizaciones de seguridad aplicadas sobre estos.
- Los responsables de los recursos físicos y/o lógicos susceptibles de actualizaciones de seguridad, deben elaborar un inventario de dichos

recursos en donde se específique los datos que permitan verificar entre otros versionamientos, finalización soporte, correlacionamiento entre recursos, etc.

- La Superintendencia Nacional de Salud, prohíbe la utilización de recursos físicos y/o lógicos obsoletos, es decir, que no cuenten con actualizaciones de seguridad y/o soporte por parte de fabricante.
- En caso de existir recursos físicos y/o lógicos en operación activa en la Superintendencia Nacional de Salud, se debe gestionar y realizar la respectiva migración de dichos recursos físicos y/o lógicos a versiones seguras.
- Así mismo, los administradores de los recursos físicos y/o lógicos susceptibles de actualizaciones de seguridad, son responsables de la inadecuada gestión sobre estos, producto de la omisión de la aplicación de las actualizaciones de seguridad y/o por la inadecuada gestión menciona anteriormente
- Cualquier excepción a la presente política de seguridad, debe ser tramitada y aprobada por medio escrito y por adelantado por el directivo responsable de la dependencia y/o proceso, quien asume la total responsabilidad de las incidencias que esta acción pueda acarrear.

5.20. Política de Seguridad de Gestión de Cambios.

La presente política de seguridad tiene como finalidad establecer los lineamientos mínimos necesarios que deben cumplir los responsables de los diferentes recursos físicos y/o lógicos, internos y/o externos en las instancias en las que se realicen modificaciones funcionales y/o de seguridad en el ecosistema digital de la Superintendencia Nacional de Salud, entre otros los siguientes:

- Los responsables de los recursos físicos y/o lógicos susceptibles de ejecutar

modificaciones que involucren el funcionamiento de los diferentes servicios prestados por la Superintendencia Nacional de Salud, tanto internos como externos, deben solicitar la debida autorización por las partes interesadas involucradas en dichos cambios.

- Los responsables de los recursos físicos y/o lógicos deben evaluar la aplicación de los diferentes cambios a realizar, en función del riesgo, criticidad y/o prioridad junto con los respectivos impactos que se puedan ocasionar sobre los usuarios que utilizan dichos recursos.
- Los responsables de los recursos físicos y/o lógicos, deben elaborar la respectiva planeación de actividades del control de cambios a aplicar, en donde evidencie entre otros los procedimientos que se llevarán a cabo para dicha acción, junto con el personal que interviene en la ejecución de la actividad y las acciones de contingencia en caso de falla.
- Todos los cambios que se realicen sobre los diferentes recursos físicos y/o lógicos, deben pasar por la debida comprobación de ejecución y funcionamiento en ambiente de pruebas, las cuales deben quedar documentadas.
- Así mismo, con las comprobaciones de ejecución y funcionamiento fallidas deben ser registradas en una base de conocimiento asociada al recurso físico y/o lógico implicado.
- Adicionalmente, los responsables de los recursos físicos y/o lógicos deben elaborar hojas de vida de los diferentes recursos en donde se evidencie las diversas actividades sobre estos, en los casos que aplique.
- Los administradores de los recursos físicos y/o lógicos, responsables de la aplicación de los cambios sobre estos, deben contar con la aprobación del líder funcional de dichos recursos según las pruebas realizas en ambientes de producción.

- Así mismo, los responsables de los recursos físicos y/o lógicos, una vez obtenida la aprobación del líder funcional, se debe contar con la debida aprobación por parte del Oficial de Seguridad de la Información junto con la debida autorización de la ejecución de los cambios por parte de la Subdirección de Tecnologías.
- Todas las implementaciones de los cambios a realizar por parte de los responsables de los recursos físicos y/o lógicos, deben realizarse en franjas de horarios en donde su impacto sea menor a través de ventanas de mantenimientos, las cuales deben ser informadas con antelación.
- En caso de existir cambios a nivel de aplicación de correcciones de seguridad que puedan afectar la confidencialidad, integridad y/o disponibilidad de los recursos físicos y/o lógicos de la Superintendencia Nacional de Salud, estas actividades tendrán prioridad alta y los respectivos involucrados en dicha gestión deben priorizar las diferentes acciones a las que haya lugar.
- Adicionalmente, todos los cambios deben ser socializados al personal involucrado y/o afectado previamente a la ejecución de dichas actividades e informar el respectivo restablecimiento de estos por los diferentes canales de comunicación oficial establecidos por la Superintendencia Nacional de Salud.
- Los responsables de los recursos físicos y/o lógicos, deber hacer seguimiento al funcionamiento de los recursos impactados producto de la implementación en ambiente producción en articulación con los líderes funcionales involucrados en la actividad, comprobando y/o validando que las modificaciones funcionan según lo proyectado.
- Una vez se finalice la validación de funcionamiento apropiado sobre los recursos impactados, se debe realizar la aceptación de conformidad por parte de los líderes funcionales de manera formal.
- Cualquier excepción a la presente política de seguridad, debe ser tramitada

y aprobada por medio escrito y por adelantado por el directivo responsable de la dependencia y/o proceso, quien asume la total responsabilidad de las incidencias que esta acción pueda acarrear.

5.21. Política de Servicios de Computación en la Nube

En la SNS, se hace necesario la contratación de recursos y servicios en la nube para que la gestión de información se efectúe de manera controlada y segura. Para tal fin, la entidad debe:

- Valorar y gestionar los riesgos de seguridad en los procesos de contratación y uso de servicios de computación en la nube asociados al tratamiento de información institucional, acceso a información personal, resistencia a ataques cometidos desde el ciberespacio, protección de secretos institucionales, riesgos legales, riesgos técnicos, riesgos de continuidad y riesgos asociados a la transmisión transfronteriza de la información institucional o personal. El análisis y gestión de los riesgos se debe realizar de acuerdo con el procedimiento de gestión de riesgos de la SNS. Los resultados del análisis y gestión de riesgos se deben documentar de acuerdo con el procedimiento de gestión de riesgo de la SNS.
- Incluir en los contratos celebrados con proveedores de servicios de computación en la nube, la necesidad de cumplir las políticas y requisitos de seguridad de la información de la SNS, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la SNS e información de carácter personal.
- Verificar que los servicios en la nube utilizados por la entidad en su operación sigan los lineamientos establecidos para la infraestructura On Premise y

desplegar validaciones de cumplimiento de seguridad basado en la ISO 27001.

- Verificar que los servicios en la nube utilizados por la entidad no almacenen o dispongan información que pueda poner en riesgo la seguridad nacional o desestabilizar las entidades del orden nacional que disponen su información para la operación de la Superintendencia.
- Identificar, gestionar y tratar los riesgos asociados al uso de servicios de computación en la nube, bajo la responsabilidad de la STI.
- Coordinar y garantizar a través de la Mesa Técnica de Seguridad de la Información, la ejecución de pruebas de seguridad tipo Ethical Hacking sobre los servicios en la nube prestados por terceros, los hallazgos encontrados en estas valoraciones de seguridad deben ser gestionados y resueltos de inmediato por parte de los proveedores de servicios cuando sea aplicable.
- Verificar que todos los usuarios de servicios de computación en la nube apliquen y cumplan los lineamientos de seguridad de la información que se definan en la SNS para el uso seguro de ese tipo de servicios de tratamiento de información.
- Controlar que los proveedores de servicios en la nube garanticen que las ubicaciones geográficas en donde se almacene información de tipo personal cuenten con leyes de protección de datos personales ampliamente aplicados sobre los procesos, instalaciones y actividades implícitas dentro de la prestación del servicio.
- Controlar que los proveedores de servicios en la nube apliquen políticas, prácticas y controles robustos de seguridad tanto al interior de sus procesos, como en la infraestructura y plataforma tecnológica sobre la cuál presten sus servicios, de igual forma, deben certificar que cuentan con las mejores prácticas internacionales de seguridad en pro de dar cumplimiento a los

requisitos de seguridad acordados contractualmente.

5.22. Política de copias de seguridad de la información.

La Superintendencia Nacional de Salud establece los siguientes lineamientos, mediante los cuales se definen los marcos de actuación y límites dentro de los cuales deben operar los funcionarios y contratistas de la Entidad en relación con la generación, gestión y uso de copias de seguridad de la información, con el fin de garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y, cuando aplique, la validez forense de los respaldos. En consecuencia, se define que:

5.22.1. Ámbito de aplicación.

Esta política aplica a todas las copias de seguridad de activos de información institucionales gestionados por la Subdirección de Tecnologías de la Información (STI), incluyendo, entre otros, servidores físicos y virtuales, máquinas virtuales, entornos de desarrollo y pruebas, funciones o servicios en la nube, sistemas de almacenamiento (storage), y demás componentes descritos en el Manual para las copias de seguridad de la información.

La política aplica a los sistemas de información misionales y críticos, así como a sus bases de datos y componentes de infraestructura asociados, de conformidad con la clasificación y priorización definida en el inventario de activos de información de la Entidad y en el “Procedimiento Copias de Seguridad SI v2”. La política aplica a los equipos de cómputo institucionales asignados a funcionarios y contratistas (estaciones de trabajo, portátiles u otros dispositivos administrados por la STI), únicamente en los casos en que se efectúen procesos de mantenimiento que impliquen reinstalación del sistema operativo o formateo de medios de almacenamiento, se gestione el retiro del funcionario o contratista de la Entidad, o se presente un incidente de seguridad o una investigación formal que requiera

preservar información contenida en dichos equipos.

Quedan excluidos de esta política, para efectos de la generación de copias de seguridad corporativas, los dispositivos personales (BYOD) y equipos no administrados por la STI, sin perjuicio de su eventual sujeción a medidas de preservación de evidencia digital en el marco de una investigación forense debidamente autorizada.

5.22.2. Herramientas y mecanismos autorizados.

Las copias de seguridad deberán realizarse exclusivamente mediante las herramientas, plataformas y servicios de respaldo de información que sean definidos, aprobados y administrados por la STI, quedando prohibido el uso de mecanismos alternos o no autorizados para generar o almacenar copias de seguridad institucionales.

La STI, a través del Grupo de Infraestructura Tecnológica (o la denominación vigente equivalente), y demás grupos internos que determine, será responsable de configurar y mantener el esquema de copias de seguridad de los servidores, sistemas de información, bases de datos, servicios en la nube y demás activos definidos en el para las copias de seguridad de la información.

5.22.3. Criterios de criticidad, alcance y frecuencia

- La STI, en coordinación con los dueños de la información y administradores funcionales de los sistemas de información, deberá garantizar la realización de copias de seguridad sobre:
  - la información y los sistemas clasificados como críticos y misionales,
  - la información institucional alojada en servidores de archivos, carpetas institucionales y repositorios corporativos definidos por la STI, y

- otros activos de información que sean priorizados en el inventario de activos debido a obligaciones legales, regulatorias o misionales.

- No será obligación de la Entidad respaldar información de usuario final almacenada en ubicaciones no institucionales o no autorizadas por la STI, ni información que no haya sido clasificada o declarada como crítica, misional o institucional de acuerdo con los lineamientos de gestión de activos de información.
- La definición de tipos de copias de seguridad (completas, incrementales, diferenciales, de logs transaccionales, imágenes de sistema, entre otras), su frecuencia, así como los medios y ubicaciones de almacenamiento, se establecerá en el Manual para las copias de seguridad de la información., los cuales deberán ser revisados y actualizados periódicamente por la STI.
- Los objetivos de punto de recuperación (RPO) y tiempo de recuperación (RTO) para cada sistema de información y base de datos deberán ser definidos por los dueños de la información y administradores funcionales, en coordinación con la STI, y documentados en los instrumentos que para tal fin disponga la Entidad.

5.22.4. Confidencialidad, integridad y disponibilidad de las copias de seguridad

Las copias de seguridad deberán almacenarse en repositorios y medios seguros, con controles de acceso basados en el principio de mínimo privilegio, de manera que solamente el personal autorizado por la STI pueda acceder, modificar, restaurar o eliminar dichos respaldos.

Cuando la naturaleza de la información lo requiera, en especial para datos personales, información reservada o clasificada y sistemas críticos, las copias de

seguridad deberán contar con mecanismos de cifrado y protección lógica que garanticen la confidencialidad de la información respaldada, de acuerdo con los lineamientos de la Política de Criptografía y las directrices de la STI.

La STI deberá garantizar la integridad de las copias de seguridad mediante la implementación de mecanismos de verificación (por ejemplo, sumas de verificación o checksums) y la ejecución de pruebas periódicas de restauración, conforme a las frecuencias y alcances definidos en el para las copias de seguridad de la información.

El esquema de respaldo deberá contemplar mecanismos de redundancia geográfica para los sistemas de información y datos críticos, ya sea mediante sitios alternos, datacenters externos o servicios en la nube que cumplan con los lineamientos de seguridad digital y continuidad de negocio adoptados por la Entidad.

5.22.5. Retención, conservación y disposición final de respaldos

Los tiempos de retención, conservación y disposición final de las copias de seguridad deberán alinearse con:

- las Tablas de Retención Documental (TRD) de la Entidad,
- la Ley General de Archivos y normas concordantes,
- la normativa de protección de datos personales y transparencia, y
- las necesidades de continuidad del negocio y recuperación ante desastres.

La determinación específica de los periodos de retención y caducidad para cada tipo de backup (diario, semanal, mensual, anual, etc.), se documenta en el Manual para las Copias de Seguridad de la Información, debiendo ser coherente con las TRD y ser aprobada por las instancias competentes de la Entidad.

La eliminación, reutilización o destrucción de medios o repositorios de respaldo deberá realizarse de forma segura, documentada y controlada, siguiendo las directrices de la STI, la normativa archivística y de protección de datos personales, de manera que se evite el acceso no autorizado o recuperación indebida de información.

5.22.6. Soporte a investigaciones y cadena de custodia de evidencia digital

Cuando una copia de seguridad pueda constituirse en evidencia digital o soporte dentro de una investigación interna, disciplinaria, administrativa o judicial, se deberán aplicar, de manera obligatoria, los procedimientos de cadena de custodia de la evidencia digital y de copias de seguridad definidos en el Manual para las copias de seguridad de la información y demás protocolos de investigación forense digital que adopte la Entidad. En estos casos, las copias de seguridad utilizadas como evidencia deberán:

- Contar con un hash criptográfico calculado mediante algoritmos reconocidos.
- Registrarse con una **estampa de tiempo cronológica** emitida por una Autoridad de Sellado de Tiempo (TSA) válida en Colombia o por los mecanismos de sello de tiempo electrónico que adopte formalmente la Entidad.
- Ser registradas en los formatos y sistemas de cadena de custodia, incluyendo como mínimo: identificación del medio o repositorio, descripción de la copia, responsables, fechas y horas de creación, traslado, acceso, análisis y, en su caso, destrucción.

La STI y el Grupo de Seguridad Digital (GSD), o la instancia que haga sus veces, deberán coordinar la aplicación de estos lineamientos con las dependencias

responsables de las investigaciones, garantizando que la gestión de copias de seguridad preserve la integridad, autenticidad, confidencialidad y trazabilidad de la evidencia digital.

5.22.7. Pruebas de restauración y verificación de efectividad

La STI deberá realizar pruebas periódicas de restauración de copias de seguridad sobre sistemas de información y bases de datos representativos, con el fin de certificar la efectividad de los respaldos, la integridad de los datos y el cumplimiento de los RPO y RTO establecidos. Los resultados de las pruebas de restauración deberán documentarse en la herramienta de gestión de TI o en los repositorios definidos por la STI, dejando evidencia de:

- el sistema o base de datos probado,
- la fecha y hora de la restauración,
- la copia utilizada,
- el responsable técnico,
- las incidencias o errores detectados, y
- las acciones de mejora implementadas.

Los administradores funcionales de los sistemas de información serán responsables de validar la funcionalidad de las aplicaciones y la integridad de la información restaurada en las pruebas y en las restauraciones reales, dejando constancia de dicha validación en los medios que defina la STI.

6. POLITICAS ESPECÍFICAS DE PRIVACIDAD DE LA INFORMACIÓN

6.1. POLÍTICA PARA LA GESTIÓN DE LA PROTECCIÓN DE DATOS PERSONALES

La Superintendencia Nacional de Salud – SNS contará con un responsable de la gestión de la protección de datos personales, quien deberá establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un Programa Integral de Gestión de Datos Personales (PIGDP) para Asegurar el cumplimiento y la gestión de los requisitos establecidos en el marco de la Ley 1581 de 2012, sus decretos reglamentarios y demás disposiciones aplicables, como parte de la responsabilidad demostrada de la SNS en materia de protección de datos personales.

Este programa garantizará la adecuada recolección y tratamiento de los datos personales, la protección eficiente y efectiva frente a las amenazas a las que pueda estar expuesta la información personal tratada en la Entidad, la garantía y desarrollo de los derechos de los titulares y, en general, la gestión de los requisitos y deberes que la SNS tiene como responsable o encargado del tratamiento de datos personales.

Lineamientos para la gestión de la protección de datos

- La SNS deberá proveer los recursos administrativos, tecnológicos, humanos y presupuestales necesarios para el diseño, implementación y seguimiento del Programa Integral de Gestión de Datos Personales.
- La SNS deberá establecer y divulgar la existencia de una dependencia, cargo o rol responsable de la adecuada gestión y cumplimiento de los requisitos internos y externos relacionados con la protección de datos personales.
- El responsable de la gestión de la protección de datos personales, con el apoyo de las diferentes áreas de la Entidad, deberá desarrollar e implementar el PIGDP, asegurando la aplicación del principio de responsabilidad demostrada.

- La Oficina Jurídica deberá realizar el monitoreo permanente de la normativa vigente en materia de protección de datos personales y alertar a la Entidad y al responsable de la gestión acerca de los cambios que sean identificados.
- La SNS podrá consultar especialistas externos cuando se requiera realizar actividades o ajustes en la protección de datos personales que superen el conocimiento del responsable y de las áreas internas de la Entidad.
- Los servidores públicos y contratistas de la SNS deberán actuar conforme a las políticas de protección de datos personales y participar activamente en las revisiones de cumplimiento que se realicen.
- Las diferentes dependencias de la SNS deberán alinear de forma periódica sus procesos y procedimientos que involucren tratamiento de datos personales, con los requerimientos normativos internos y externos relacionados con seguridad y privacidad de la información.
- El responsable de la gestión de la protección de datos personales, con el apoyo de la Oficina Jurídica, brindará acompañamiento a las áreas internas de la Entidad cuando estas requieran realizar actividades de recolección o tratamiento de datos personales.
- El responsable, con el apoyo de la Oficina Jurídica, la Oficina de Tecnologías de la Información y la Oficina de Comunicaciones, deberá desarrollar y socializar directrices internas que regulen el tratamiento de datos personales dentro de la Entidad.
- El responsable de la gestión de la protección de datos personales definirá o revisará la documentación necesaria para demostrar el cumplimiento normativo en protección de datos personales en la SNS.
- El responsable establecerá los lineamientos, herramientas o instrumentos que permitan determinar el nivel de cumplimiento de los encargados o terceros que realicen tratamiento de datos personales en nombre de la

Entidad.

- Las dependencias de la SNS, con el apoyo del responsable de protección de datos, deberán identificar y evaluar los riesgos asociados al tratamiento, transmisión o transferencia de datos personales.
- El responsable velará porque dentro del Plan General de Auditoría de la Entidad se incluya la revisión de los aspectos técnicos, jurídicos y procedimentales relacionados con la protección de datos personales.
- El responsable de la gestión de la protección de datos personales deberá evaluar el cumplimiento, resultados y documentación de las acciones correctivas y/o preventivas relacionadas con el tratamiento de datos personales.

6.2. POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES

La Superintendencia Nacional de Salud – SNS, en cumplimiento del principio de legalidad establecido en la Ley 1581 de 2012, sus decretos reglamentarios y demás disposiciones en materia de protección de datos personales, adoptará los requisitos, mecanismos y controles apropiados para garantizar la protección, privacidad y buen uso de la información personal de los titulares.

La SNS reconoce que los datos personales son información protegida por la normativa vigente en Colombia y por convenios internacionales, y que su tratamiento debe realizarse en condiciones de legalidad, transparencia, finalidad y proporcionalidad, asegurando siempre el respeto por los derechos fundamentales de los titulares.

Lineamientos para el tratamiento de datos personales

- Las dependencias, direcciones, oficinas o áreas de la SNS que en el ejercicio de sus funciones recolecten datos personales deberán diseñar, implementar y divulgar los avisos de privacidad y las autorizaciones de tratamiento en los respectivos medios de captura.
- Los servidores públicos y contratistas, con el apoyo del responsable de la gestión de protección de datos personales, deberán asegurar que los avisos de privacidad cumplan, como mínimo, con la estructura establecida en la normativa aplicable.
- Todo proceso de recolección y tratamiento de datos personales deberá cumplir estrictamente con los requisitos legales y lineamientos internos definidos por la SNS.
- En toda recolección de datos personales se deberá solicitar y conservar prueba de la autorización otorgada por el titular, salvo en los casos en que la Ley prevea excepciones.
- La información personal tratada por la SNS solo podrá usarse para las finalidades previamente informadas y autorizadas por los titulares, quedando expresamente prohibido cualquier uso distinto, en especial el uso comercial o privado no autorizado.
- Ninguna persona podrá realizar tratamiento de datos personales sin contar con la autorización previa, expresa e informada del titular, salvo en los casos de excepción previstos por la Ley.
- El tratamiento de datos de niños, niñas y adolescentes deberá realizarse únicamente con la autorización de sus padres, tutores o representantes legales, y siempre que dicho tratamiento responda y respete el interés superior de los menores y asegure el respeto de sus derechos fundamentales.

6.3. POLÍTICA PARA LA GESTIÓN DE DERECHOS DE LOS TITULARES

La Superintendencia Nacional de Salud – SNS respetará y garantizará que los titulares de datos personales puedan ejercer en todo momento sus derechos de conocer, actualizar, rectificar sus datos personales, así como solicitar prueba de la autorización otorgada, ser informados sobre el uso que se dará a su información, y revocar la autorización o solicitar la supresión de sus datos cuando el tratamiento no respete los principios, derechos y garantías establecidos por la Ley.

Lineamientos para la gestión de derechos de los titulares

- La SNS garantizará que toda consulta, solicitud de rectificación, actualización o supresión sea atendida dentro de los plazos legales previstos en la normativa vigente.
- Los servidores públicos y contratistas de la SNS deberán abstenerse de responder directamente consultas o reclamaciones relacionadas con protección de datos personales sin la intervención y coordinación del responsable de la gestión de la protección de datos personales.
- Los funcionarios responsables de los canales de atención habilitados para el ejercicio de derechos de los titulares deberán mantener su disponibilidad, accesibilidad y correcto funcionamiento, de manera que permitan el ejercicio efectivo de los derechos de los ciudadanos.
- Cualquier solicitud, consulta o reclamo relacionado con la protección de datos personales deberá ser comunicado de forma inmediata al responsable de la gestión de protección de datos personales.
- El responsable de la gestión de la protección de datos personales deberá velar por la existencia y actualización de un registro de consultas y reclamaciones, en el cual se documente el estado y resultado de cada

solicitud recibida.

- La SNS y el responsable de la gestión de protección de datos deberán asegurar que todas las solicitudes o reclamaciones recibidas sean atendidas y respondidas de manera formal, incluso en aquellos casos en los que los datos personales del solicitante no se encuentren registrados en las bases de datos de la Entidad.
- Los servidores públicos y contratistas de la SNS deberán abstenerse de eliminar, suprimir, modificar u omitir cualquier consulta, reclamo o solicitud de protección de datos personales presentada por los titulares.
- La SNS destinará por lo menos un suplente para el responsable de la gestión de la protección de datos personales, quien será responsable como mínimo de atender y hacer seguimiento al cumplimiento en la atención de consultas en aquellos casos en los cuales el responsable principal no se encuentre habilitado para realizar sus funciones.

6.4. POLÍTICA PARA EL TRATAMIENTO DE DATOS SENSIBLES

La Superintendencia Nacional de Salud – SNS reconoce que ciertos datos personales tienen una especial categoría de protección por las consecuencias negativas que puede generar su inadecuado tratamiento. La Ley ha definido como datos sensibles aquellos relacionados con el origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales o de derechos humanos, datos relativos a la salud, la vida sexual, datos biométricos y la información de niños, niñas y adolescentes.

Por regla general, estos datos solo podrán ser objeto de tratamiento cuando el titular otorgue su autorización previa, expresa e informada, o cuando se configure alguna de las excepciones legales previstas.

La SNS implementará procedimientos y controles formales que fortalezcan la protección de los datos personales sensibles en todas las actividades que involucren su recolección, almacenamiento, uso, circulación, comunicación, transmisión, intercambio o transferencia.

Lineamientos para el tratamiento de datos sensibles

El tratamiento de datos sensibles en la SNS estará prohibido, salvo cuando:

- El titular otorgue su autorización previa, expresa e informada, salvo en los casos en que por Ley no se requiera.
- El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado; en tales casos, la autorización deberá ser otorgada por sus representantes legales.
- El tratamiento sea realizado en el curso de las actividades legítimas de una organización sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera únicamente a sus miembros o personas con contacto regular en virtud de su objeto. En estos eventos, los datos no podrán suministrarse a terceros sin autorización del titular.
- El tratamiento se refiera a datos necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga finalidades históricas, estadísticas o científicas, siempre que se adopten las medidas conducentes a la supresión de la identidad de los titulares.
- El responsable de la gestión de la protección de datos personales deberá proporcionar o coordinar la capacitación específica dirigida a las

dependencias, áreas o funcionarios que requieran realizar tratamiento de datos sensibles.

- Todo servidor público, contratista o tercero que requiera recolectar datos sensibles en la SNS deberá garantizar que dicha recolección se realice únicamente a través de mecanismos que aseguren la obtención válida de la autorización expresa del titular.

6.5. POLÍTICA PARA EL REGISTRO E INVENTARIO DE BASES DE DATOS

El Registro Nacional de Bases de Datos – RNBD es el directorio público de las bases de datos sujetas a tratamiento que operan en el país. Este registro es administrado por la Superintendencia de Industria y Comercio (SIC) y es de libre consulta para los ciudadanos.

El Gobierno Nacional, a través del Capítulo 26 del Decreto Único 1074 de 2015, reglamentó la información mínima que debe contener el RNBD, así como los términos y condiciones bajo los cuales se deben inscribir las bases de datos sujetas a la aplicación de la Ley 1581 de 2012.

En consecuencia, la Superintendencia Nacional de Salud – SNS establecerá procedimientos y controles formales que aseguren la identificación, inventario y actualización oportuna de la información de sus bases de datos en la plataforma del RNBD, conforme a los plazos legales aplicables, con el fin de evitar sanciones, multas, suspensión de actividades o cierres derivados del incumplimiento normativo.

Lineamientos para el registro e inventario de bases de datos

- Una vez identificadas, la SNS deberá registrar en el RNBD las nuevas bases de datos que cree o gestione, así como reportar cualquier cambio o actualización que se presente en aquellas previamente inscritas.
- Todas las dependencias, direcciones, oficinas o grupos de la SNS deberán apoyar al responsable de la gestión de la protección de datos personales en la identificación, consolidación y actualización de la información requerida para el registro.
- El registro de las bases de datos deberá realizarse de manera completa, transparente y veraz, sin omitir intencionalmente bases de datos, tratamientos, finalidades o categorías de información personal que reposen en los sistemas de la Entidad.
- El responsable de la gestión de la protección de datos personales, o quien se designe formalmente, será el encargado de realizar el registro, actualización o eliminación de las bases de datos en la plataforma del RNBD ante la SIC.
- La SNS garantizará que el registro y actualización de sus bases de datos se realice siempre dentro de los términos y condiciones legales vigentes, asegurando trazabilidad documental y responsabilidad demostrada en el cumplimiento de esta obligación.

6.6. POLITICA PARA LA RECOLECCIÓN DE DATOS PERSONALES

La recolección de datos personales en la Superintendencia Nacional de Salud – SNS se llevará a cabo mediante métodos y procedimientos lícitos y legítimos, en concordancia con lo dispuesto en la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa vigente en materia de protección de datos personales. Estos

lineamientos buscan garantizar que la información recolectada responda a finalidades específicas, legítimas y previamente informadas, respetando en todo momento los derechos y libertades de los titulares, es por ello que en el presente numeral se establecen lineamientos claros que permitan una recolección transparente, segura y conforme a los principios de privacidad, legalidad, finalidad, libertad, veracidad, necesidad, proporcionalidad y confidencialidad que rigen el tratamiento de datos personales en Colombia.

Lineamientos frente a la recolección

- La SNS deberá obtener el consentimiento previo, expreso, informado y libre de los titulares antes de recolectar sus datos personales, salvo las excepciones establecidas por la Ley.
- No se podrá recolectar información personal sin una base legal válida o sin el consentimiento del titular, salvo que exista una excepción legal aplicable.
- La recolección de datos sensibles solo podrá realizarse en los casos expresamente permitidos por la Ley y siempre con la autorización explícita del titular.
- La recolección de datos deberá ajustarse a los principios de finalidad, necesidad y proporcionalidad, es decir, solo se podrán recolectar los datos estrictamente necesarios para fines legítimos, específicos y previamente informados.
- Los titulares deberán ser informados de manera clara y accesible sobre los propósitos del tratamiento, sus derechos y los mecanismos dispuestos para ejercerlos.
- La SNS deberá implementar y mantener medidas de seguridad técnicas, administrativas y físicas para proteger los datos recolectados frente a

accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas.

- Los mecanismos para obtener el consentimiento de los titulares deberán ser claros, verificables y accesibles, tales como formularios de autorización o declaraciones de privacidad.
- Se deberá establecer un sistema de registro y trazabilidad que documente el modo, medio y circunstancias bajo las cuales se obtuvo el consentimiento.
- La información recolectada deberá mantenerse actualizada, adoptando medidas razonables para su corrección o rectificación cuando sea necesario.
- La SNS deberá garantizar la confidencialidad de los datos personales recolectados y abstenerse de utilizarlos para fines diferentes a los autorizados por el titular.
- Antes de recolectar datos sensibles, deberá identificarse la necesidad de su tratamiento e informar de forma expresa al titular sobre esta circunstancia, advirtiendo la obligatoriedad de una autorización explícita.
- La recolección de información deberá realizarse únicamente a través de los canales físicos o digitales autorizados por la SNS, aplicando los estándares definidos en materia de seguridad y protección de datos.

6.7. POLITICA PARA EL ALMACENAMIENTO DE DATOS PERSONALES

El almacenamiento de datos personales en la Superintendencia Nacional de Salud – SNS se centra en la implementación de métodos y procedimientos que aseguren la custodia segura, confiable y responsable de la información recolectada. El propósito principal es proteger la integridad, confidencialidad y disponibilidad de los datos personales mediante la aplicación de medidas de seguridad técnicas, jurídicas y administrativas que prevengan accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas. Con este numeral se busca establecer

prácticas responsables de almacenamiento que garanticen el cumplimiento de la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa vigente, asegurando a su vez la protección efectiva de los derechos de los titulares.

Lineamientos frente al almacenamiento

- La SNS deberá asegurar el cumplimiento de los principios fundamentales del tratamiento de datos personales, incluyendo legalidad, finalidad, libertad, transparencia, veracidad, acceso y circulación restringida, seguridad, necesidad, minimización, integridad, confidencialidad y limitación temporal de almacenamiento.
- El acceso a los datos personales almacenados deberá ser estrictamente restringido. Solo estarán autorizadas las personas que requieran la información para el desarrollo de sus funciones, bajo criterios de necesidad y proporcionalidad.
- Se deberá garantizar la confidencialidad de los datos personales almacenados, prohibiéndose su divulgación a terceros no autorizados.
- Los datos personales almacenados deberán ser utilizados únicamente para las finalidades legítimas y previamente informadas al titular. Su uso para fines distintos o no autorizados estará prohibido, salvo que exista justificación legal o consentimiento expreso del titular.
- La SNS deberá aplicar de manera obligatoria las medidas de seguridad establecidas, incluyendo controles de acceso, uso de contraseñas seguras, cifrado de datos, sistemas de detección y prevención contra programas maliciosos, copias de seguridad y demás prácticas de seguridad de la información. Las copias de seguridad que contengan datos personales se gestionarán de acuerdo con la Política de copias de seguridad de la

información (5.20) y las normas de protección de datos personales aplicables.

- Los datos personales almacenados deberán mantenerse exactos, completos y actualizados. Cualquier inexactitud o cambio deberá ser informado de inmediato al responsable de protección de datos personales para su corrección o actualización.
- La SNS deberá establecer y respetar plazos de conservación y retención de datos personales, conforme a lo dispuesto en la Ley, en la normatividad sectorial y en las tablas de retención documental de la entidad.
- Se deberá garantizar que únicamente se almacenen los datos personales estrictamente necesarios y pertinentes para el cumplimiento de las finalidades autorizadas, evitando acumulaciones innecesarias de información.

6.8. POLITICA DE USO DE DATOS PERSONALES

El uso de los datos personales en la Superintendencia Nacional de Salud – SNS se refiere a la forma en que la entidad debe manejar y emplear la información personal recolectada, garantizando que su tratamiento se realice de manera responsable, ética, legal y transparente. Este apartado establece los principios y prácticas esenciales que aseguran que el uso de los datos personales cumpla con los fines autorizados por los titulares, dentro de los marcos de legalidad, finalidad, necesidad y proporcionalidad, y con el respeto pleno a los derechos fundamentales de los ciudadanos. Asimismo, se establecen medidas de seguridad y controles internos que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la información durante todo su ciclo de vida.

Lineamientos frente al uso de datos personales

- La SNS deberá obtener el consentimiento previo, expreso, informado y libre de los titulares antes de recopilar, utilizar o divulgar sus datos personales, salvo en los casos de excepción previstos en la Ley.
- El consentimiento deberá cumplir con la estructura mínima legalmente exigida, garantizando que sea específico, informado y voluntario.
- El uso de los datos personales deberá limitarse estrictamente a la finalidad específica para la cual fueron recolectados, previamente informada al titular. Cualquier uso distinto requerirá una nueva autorización expresa del titular.
- La SNS deberá garantizar que los datos personales utilizados se mantengan exactos, completos y actualizados, adoptando medidas razonables para corregir, rectificar o eliminar información inexacta o desactualizada.
- La entidad no podrá utilizar datos personales sin contar con una base legal válida o sin la autorización previa del titular, salvo en los casos de excepción legal previstos en la normativa vigente.

6.9. POLITICA DE CIRCULACIÓN DE DATOS PERSONALES

La circulación de datos personales en la Superintendencia Nacional de Salud – SNS comprende las actividades de transferencia, transmisión, intercambio o comunicación de información personal dentro de la Entidad, hacia otras entidades públicas o privadas, o incluso hacia el exterior del país. Este proceso debe garantizarse bajo condiciones de legalidad, transparencia, seguridad y proporcionalidad, respetando siempre los derechos de los titulares e implementando medidas de control que prevengan accesos indebidos o tratamientos no autorizados. El presente numeral establece los lineamientos y obligaciones que deben observarse para asegurar una circulación responsable y segura de los datos personales, desde la obtención del consentimiento informado hasta la adopción de

medidas contractuales, técnicas y organizacionales adecuadas.

Lineamientos frente a la circulación de datos

- La SNS deberá obtener el consentimiento previo, expreso, informado y libre de los titulares cuyos datos personales serán objeto de circulación, informando con claridad los fines, el alcance y los destinatarios de dicha circulación.
- La circulación de datos personales deberá estar limitada a la finalidad legítima y específica para la cual fueron recolectados, quedando prohibido cualquier uso no autorizado, incompatible o ajeno a los fines inicialmente informados.

- Cuando el titular lo solicite, la SNS deberá informar las circunstancias y condiciones en las que se realizará la circulación de sus datos personales, incluyendo la identificación de los terceros involucrados y las medidas de seguridad aplicadas.
- Se deberán establecer de manera obligatoria acuerdos de confidencialidad y cláusulas contractuales con terceros receptores de datos, para asegurar que estos los protejan adecuadamente y los utilicen únicamente para los fines autorizados.
- En los casos en que se realicen transferencias internacionales de datos personales hacia países que no ofrezcan un nivel adecuado de protección, la SNS deberá solicitar autorización previa a la Superintendencia de Industria y Comercio (SIC), en los términos establecidos por la normativa vigente.
- Toda transferencia o transmisión de datos personales deberá estar respaldada por la adopción de salvaguardias adecuadas, tales como

cláusulas contractuales, contratos de transmisión, acuerdos de confidencialidad u otros mecanismos que garanticen el cumplimiento de la normativa.

- La SNS deberá asegurar en todo momento el respeto y garantía de los derechos de los titulares en relación con la circulación de sus datos personales, incluyendo los derechos de acceso, rectificación, supresión y oposición (ARCO).

6.10. POLITICA DE SUPRESIÓN DE DATOS PERSONALES

La supresión de datos personales en la Superintendencia Nacional de Salud – SNS constituye un procedimiento esencial dentro del ciclo de vida de la información, mediante el cual se eliminan de forma segura, definitiva e irreversible los datos personales que ya no son necesarios o cuya conservación ha vencido, en cumplimiento de lo dispuesto en la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa aplicable. Este proceso tiene como finalidad garantizar el derecho a la privacidad de los titulares, asegurar el cumplimiento de los principios de necesidad, finalidad y proporcionalidad, y mitigar riesgos asociados al almacenamiento o uso indebido de datos personales que no deben continuar siendo tratados.

Lineamientos frente a la supresión de datos personales

- La SNS deberá realizar revisiones periódicas de sus bases de datos para identificar los registros que deban ser suprimidos, de acuerdo con los criterios legales, contractuales o institucionales de conservación.
- Antes de eliminar un dato personal, se deberá verificar que ya no sea necesario para la finalidad para la cual fue recolectado o que haya expirado

el plazo legal o documental de conservación.

- La supresión de datos deberá llevarse a cabo aplicando medidas técnicas y organizativas de seguridad, garantizando que la eliminación sea definitiva e irreversible, evitando toda posibilidad de recuperación posterior.
- En los casos en que los datos personales hayan sido compartidos con terceros (encargados o aliados), la SNS deberá notificarles la supresión y exigir la eliminación correspondiente en sus propios sistemas.
- La Entidad deberá mantener un registro documental y trazable de todas las actividades de supresión de datos, incluyendo fechas, responsables, justificación legal y evidencias de ejecución.
- Deberán conservarse registros administrativos que respalden la eliminación realizada, a efectos de demostrar cumplimiento bajo el principio de responsabilidad demostrada.
- En los casos en que el tratamiento de datos se hubiera realizado con consentimiento del titular, la SNS deberá informarle de manera clara y transparente sobre la supresión efectuada, asegurando su derecho a conocer el destino final de su información personal.
- Una vez cumplida la finalidad del tratamiento, la SNS deberá procurar la eliminación o, en su defecto, la anonimización de los datos, siempre que esta última garantice la imposibilidad de identificar directa o indirectamente a los titulares.

Control de cambios					
Elaboró		**Revisó**		**Aprobó**	
Nombre	1.Jose Luis Alejandro Carrillo Valderrama 2. Milsora Gómez Damian 3. Leonardo Santos Chacón	**Nombre**	Omar Fredy García Ortega	**Nombre**	Jose Alexander de los Reyes
Cargo	1. Profesional Especializado 2. Profesional Especializado 3. Contratista	**Cargo**	Subdirector Técnico Subdirección de Tecnologías de la Información	**Cargo**	Director Dirección de Innovación y Desarrollo
Fecha	01 de Febrero de 2026	**Fecha**	16 de Febrero de 2026	**Fecha**	20 de Febrero de 2026