REPÚBLICA DE COLOMBIA

Libertad y Orden

INSTITUTO NACIONAL DE SALUD

RESOLUCIÓN NÚMERO 0002 **DE 2026**

(05 ENE 2026)

"Por la cual se designa al Oficial de Seguridad y Privacidad de la Información y Seguridad Digital del Instituto Nacional de Salud"

LA DIRECTORA GENERAL DEL INSTITUTO NACIONAL DE SALUD

En ejercicio de sus facultades legales contempladas en el numeral 23 del artículo 5 del Decreto 2774 de 2012 y

CONSIDERANDO

Que la Constitución Política en su artículo 15 consagra el derecho fundamental que tienen todas las personas a conservar su intimidad personal y familiar, al buen nombre, conocer, actualizar y rectificar la información que se haya recogido sobre ellos en los bancos de datos y en archivos de entidades públicas y privadas.

Que el Instituto Nacional de Salud – INS es un instituto científico y técnico, con personería jurídica, autonomía administrativa y patrimonio propio, cuya estructura interna se define en el Decreto 2774 de 2012.

Que el INS, en su carácter de autoridad científico-técnica, tiene como objeto, entre otros, la gestión del conocimiento científico en salud y biomedicina, la vigilancia y seguridad sanitaria en temas de su competencia, la producción de insumos biológicos, y actuar como laboratorio nacional de referencia y coordinador de redes especiales, lo cual demanda medidas reforzadas de seguridad y privacidad de la información institucional.

Que, para el cumplimiento de su objeto y funciones, el INS participa en la planeación, desarrollo y coordinación de sistemas de información en salud pública, lo cual implica gestión integral de riesgos y controles sobre la información institucional y los datos personales tratados por la entidad.

Que de conformidad con el Decreto 2774 de 2012, el INS cuenta con Direcciones misionales tales como Dirección de Investigación en Salud Pública, Dirección de Vigilancia y Análisis del Riesgo en Salud Pública, Dirección de Redes en Salud Pública y Dirección de Producción, además de las subdirecciones misionales asociadas, cuya operación se apalanca en activos de información y servicios tecnológicos críticos que requieren lineamientos transversales de seguridad y privacidad.

Que la Oficina de Tecnologías de la Información y las Comunicaciones tiene, de forma general, entre sus funciones, proponer políticas TIC, asegurar la consistencia y seguridad de datos e información institucional y atender e implementar políticas y acciones relativas a la seguridad de la información y de la plataforma tecnológica del Instituto, razón por la cual su jefatura constituye un rol idóneo para ejercer la función transversal de Oficial de Seguridad y Privacidad de la Información y Seguridad Digital.

Que el artículo 25 de la Ley 1581 de 2012 creó el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio, y se han impartido instrucciones para su gestión mediante la Circular Única / circulares externas de la SIC.

Que el Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG) en el numeral 3.4.2 Política de Seguridad Digital - Lineamientos generales para la implementación, establece (...) *"se debe articular los esfuerzos, recursos, metodologías*

y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la Alta Dirección" (...).

Que el Manual de Gobierno Digital, del que trata el Decreto 1008 de 2018 (cuyas disposiciones se encuentran compiladas en el Decreto 1078 de 2015, capítulo 1, título 9, libro 2, parte 2), establece en el numeral 1.6. los Roles e instancias importantes para la implementación de la política, entre los cuales se encuentra el responsable de Seguridad de la Información, en el cual se dicta que (...) en la respectiva entidad, se debe designar un responsable de Seguridad de la Información que a su vez responderá por la Seguridad Digital en la entidad, el cual debe pertenecer a un área que haga parte del direccionamiento estratégico o Alta Dirección (...).

Que el Decreto 1008 de 2018, el cual establece los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, determina que (...) "la seguridad de la información busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano"(...).

Que, el Ministerio de Tecnologías de la Información y las Comunicaciones estableció, a través de la Resolución 500 de 2021 los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI, como habilitador de la política de Gobierno Digital, el cual conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Que mediante la adopción del Modelo de Seguridad y privacidad por parte de las entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de seguridad de la información, cumpliendo con la aplicación del concepto de Seguridad Digital.

Que mediante la Resolución 1457 de 2025 el Instituto Nacional de Salud actualiza la Política de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la operación de los servicios tecnológicos como uno de los habilitadores de la política de Gobierno Digital, así como las políticas generales de manejo y los lineamientos frente a su uso y administración, con el fin de garantizar la protección de los activos de información, la prestación continua de los servicios institucionales, la seguridad de los datos de terceros obtenidos bajo el desarrollo de las actividades misionales y el cumplimiento de los principios de confidencialidad, integridad, privacidad y disponibilidad de la información.

Que por todo lo anterior el Instituto Nacional de Salud requiere designar el Oficial de Seguridad y privacidad de la Información y de Seguridad Digital, definir las responsabilidades para la implementación de la política de seguridad digital, para dar cumplimiento al Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC, habilitador transversal de la Política de Gobierno Digital.

Que, en mérito de lo expuesto,

"Por la cual se designa al Oficial de Seguridad y Privacidad de la Información y Seguridad Digital del Instituto Nacional de Salud"

RESUELVE

ARTÍCULO 1. Designar al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, el rol de Oficial de Seguridad y Privacidad de la Información y Seguridad Digital.

ARTÍCULO 2. El funcionario delegado, en su rol de Oficial de Seguridad y Privacidad de la Información y de Seguridad Digital, tendrá a su cargo las siguientes funciones:

Respecto a Seguridad y Privacidad de la Información:

1. Fomentar la implementación del habilitador transversal de seguridad y privacidad de la Política de Gobierno Digital y la política de Seguridad Digital al interior del INS.
2. Asesorar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y seguridad digital (ciberseguridad) para la misma, de conformidad con la regulación vigente.
3. Identificar y gestionar la brecha de Seguridad y privacidad de la información y seguridad digital entre el MSPI y la situación actual de la Entidad.
4. Realizar la estimación, planificación y cronograma de la implementación del MSPI.
5. Liderar la implementación y hacer seguimiento a las tareas y cronograma definido del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad.
6. Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.
7. Liderar y brindar acompañamiento a los procesos de la Entidad en la gestión de riesgos de seguridad y privacidad de la información y seguridad digital (ciberseguridad), así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
8. Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información y seguridad digital.
9. Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización, concienciación y divulgación de la seguridad y privacidad de la información para servidores públicos y contratistas.
10. Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información y seguridad digital (ciberseguridad).
11. Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad y privacidad de la información y seguridad digital en la entidad.
12. Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información y seguridad digital (ciberseguridad).
13. Poner en conocimiento de las dependencias con competencia funcional, cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información y seguridad digital (ciberseguridad) de acuerdo con la normativa vigente.
14. Reportar al Registro Nacional de Bases de Datos (RNBD) de la Superintendencia de Industria y Comercio (SIC) o quien haga sus veces, de conformidad con lo dispuesto en la norma, las bases de datos con datos personales que reposan en la Entidad.
15. Atender, en representación de la Entidad, las visitas de inspección y los requerimientos que realice la autoridad designada para la verificación del cumplimiento del MSPI y de la Ley de protección de datos personales.
16. Mantener y documentar los contactos con autoridades (policía Nacional, INTERPOL, Bomberos, Defensa Civil, Grupos de atención de desastres, SIC, etc.)

u otros especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad y privacidad de la información que requiera de asesoría externa.

17. Mantener contacto con grupos de interés especializados en seguridad y privacidad de la información y seguridad digital, con el fin de compartir e intercambiar conocimientos en pro a la mejora continua del MSPI de la Entidad.
18. Reportar al Comité Directivo el estado de la implementación del MSPI.
19. Atender las peticiones, quejas, reclamos, sugerencias y denuncias (PQRSD) en materia de seguridad y privacidad de la información, seguridad digital.
20. Asistir a los eventos en representación de la Entidad que le sean designados por el despacho de la Dirección.
21. Coordinar el equipo de trabajo de gestión e implementación en seguridad y privacidad de a información y seguridad digital al interior de la Entidad.
22. Participar en las mesas de trabajo del Comando Conjunto de Operaciones Cibernéticas e Infraestructuras Críticas Cibernéticas Nacionales (CCOCI) del país y en aquellas mesas de trabajo que designe el Despacho de la Dirección.
23. Revisar y verificar el cumplimiento de los requisitos legales y reglamentarios en materia de Seguridad y Privacidad de la Información y seguridad digital.
24. Liderar en conjunto con los líderes de proceso, la actualización y publicación de los instrumentos de gestión de la información, en conjunto con sus respectivos actos administrativos, en atención a los lineamientos dispuestos por la Ley 1712 de 2014 y el anexo 2 de la Resolución 1519 de 2020 de MinTIC.
25. Aplicar los estándares mínimos técnicos y de seguridad digital aplicables a los sujetos obligados en sus sitios web, definidas en el Anexo 3 de la Resolución 1519 de 2020 de MinTIC.
26. Realizar seguimiento a las vulnerabilidades identificadas en la plataforma tecnológica de la entidad y sistemas de información, y coordinar los respectivos planes de remediación de acuerdo con los resultados obtenidos

ARTÍCULO 3. Ámbito de aplicación. Las disposiciones mencionadas en la presente resolución serán aplicables a todos los procesos del Instituto Nacional de Salud, en atención a los lineamientos emitidos por el Oficial de Seguridad y Privacidad de la Información y Seguridad Digital.

ARTÍCULO 4. Responsabilidades de los propietarios de los activos de información. El propietario del activo de información corresponde al nombre del cargo, dependencia, o al nombre de la entidad externa quien decide sobre el activo de información, establece controles, lo modifica, crea, cambia, ajusta, elimina o transforma, el cual deberá:

1. Dar cumplimiento a las políticas de seguridad y privacidad de la información y seguridad digital establecidas.
2. Definir el nivel de clasificación y criticidad de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida de este.
3. Informar al Oficial de Seguridad y Privacidad de la Información y Seguridad Digital, cuando detecte cualquier incidente, para que sea tratado y corregido mediante la aplicación de controles.
4. Implementar las medidas de seguridad y privacidad de la información necesarias en su área para evitar eventos, incidentes de seguridad o violaciones a la privacidad de los activos de información.
5. En los casos en que aplique, asegurarse de que el personal (servidores públicos, contratistas o proveedores) tenga cláusulas de confidencialidad en los contratos y sea consciente de sus responsabilidades.

"Por la cual se designa al Oficial de Seguridad y Privacidad de la Información y Seguridad Digital del Instituto Nacional de Salud"

ARTÍCULO 5. Responsabilidades de los usuarios de la información. Se entiende por usuario de la información cualquier servidor público, contratista, proveedor o tercero, que utiliza la información procesada y suministrada por el INS para ejercer sus funciones o actividades contratadas en las dependencias y procesos de la entidad, y tienen responsabilidad de:

1. Conocer, comprender y aplicar las políticas de seguridad y privacidad de la información y seguridad digital establecidas por el INS.
2. Participar en las campañas de sensibilización, concienciación y capacitación en seguridad y privacidad de la información y seguridad digital del INS.
3. Aplicar las medidas de protección de la información a su cargo, de acuerdo con su clasificación y valor para garantizar la confidencialidad, integridad, privacidad y disponibilidad de la información.
4. Reportar las debilidades, eventos, riesgos o los incidentes de seguridad identificados en la operación de su proceso, a través de la mesa de ayuda, según lo establecido en el procedimiento.
5. Cumplir con el acuerdo de confidencialidad y manejo de la información firmado con la entidad.

ARTÍCULO 6. Vigencia. La presente resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 5 días del mes de enero de 2026

DIANA MARCELA PAVA GARZÓN
Directora General

Revisó: Carlos Andrés López Fernández - Jefe OTIC
Proyectó: Sergio Andrés Ramos P - Contratista OTIC