REPÚBLICA DE COLOMBIA

Libertad y Orden

INSTITUTO NACIONAL DE SALUD

RESOLUCIÓN NÚMERO 1457 **DE** 2025

(04 DIC 2025)

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

LA DIRECTORA GENERAL DEL INSTITUTO NACIONAL DE SALUD

En ejercicio de sus facultades legales contempladas en los numerales 23, 29 y 35 del artículo 5 del Decreto 2774 del 2012 y,

CONSIDERANDO

Que el artículo 15 de la Constitución Política, establece el fundamento principal de la seguridad y privacidad de la información digital consagrando el derecho fundamental al Habeas Data, según el cual (..) "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".

Que la Ley 527 de 1999 (..) "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

Que el Decreto 1078 de 2015 Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, dispone en el artículo 2.2.9.1.2.1 que la Política de Gobierno Digital será definida por el MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, dispone que los habilitadores transversales de la Política de Gobierno Digital, corresponde a las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital y están compuestos por Arquitectura, Cultura y Apropiación, Seguridad y privacidad de la Información y Servicios Ciudadanos Digitales.

Que el Título 9, Políticas y Lineamientos de Tecnologías de la Información, Capítulo 1 del Decreto 1078 de 2015, Subrogado por el artículo 1 del Decreto 767 de 2022, Política de Gobierno Digital, artículo 2.2.9.1.1.2. establece que "Los sujetos obligados a las disposiciones contenidas en el presente capítulo serán las entidades que conforman la administración pública en los términos del artículo 39 de la Ley 489 de 1998 (...)".

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

Que el Decreto 767 de 2022 "Por el cual se establecen 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 1078 de 2015, Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" dispone al tenor del numeral 3.2 del artículo 2.2.9.1.2.1. que el habilitador transversal de la Política de Gobierno Digital, Seguridad y Privacidad de la Información "(...) busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.".

Que para desarrollar el habilitador transversal de "Seguridad y Privacidad de la Información" el MINTIC expidió la Resolución 00500 de 2021 que establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establece los lineamientos y estándares para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015.

Que el artículo 5 de la norma en cita, establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital.

Dicha estrategia debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue; como el Modelo de Seguridad y Privacidad de la Información – MSPI señalado en el Anexo 1 de la misma resolución, como habilitador de la política de Gobierno Digital, actualizado con la resolución 02277 de 2025.

Que la Resolución 746 de 2022 del MinTIC, establece lineamientos adicionales a los establecidos en la Resolución número 500 de 2021, fortaleciendo el Modelo de Seguridad y Privacidad de la Información en los términos de adoptar medidas, al momento de adquirir productos y servicios de Seguridad Digital operados en entornos de nube, que garanticen el cumplimiento de lo dispuesto en la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias, en particular las relativas a la transferencia internacional de datos personales, así como la gestión de la seguridad de la información para las relaciones con los proveedores, determinando e implementando los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital.

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

Que mediante Resolución 0661 de 2021 el INS actualizó la operación del Sistema de Gestión de Calidad y su articulación con los demás sistemas implementados acorde al alcance definido en el MNL-D02.0000-001 Manual del SIG incluida la NTC-ISO/IEC 27001 de seguridad de la información.

Que, mediante Resolución 0839 de 2025 el INS actualizó la Política de Seguridad y Privacidad de la Información. Sin embargo, la Oficina de Tecnologías de Información y Comunicaciones - OTIC, en el marco de la evaluación de dicha política y la evolución del marco normativo recomendó articularla teniendo en cuenta la actualización a la versión 2022 de la NTC-ISO/IEC 27001 base para la implementación del SGSPI, incluyendo buenas prácticas de seguridad digital para el manejo de los sistemas y tecnologías de información en la entidad, medidas de seguridad y privacidad efectivas para garantizar la integridad, confidencialidad, privacidad y disponibilidad de la información, lo que permite prevenir y gestionar riesgos asociados al uso del ciberespacio, la inteligencia artificial y de las herramientas tecnológicas en el cumplimiento de los objetivos de la entidad.

Por tanto, y de conformidad con la necesidad expuesta, en sesión extraordinaria del noviembre 13 de 2025 fue puesta en consideración del Comité Institucional de Gestión y Desempeño la actualización de la Política de Seguridad y Privacidad de la información y Seguridad Digital, como uno de los elementos habilitadores de la Política de Gobierno Digital, así como la derogatoria de la Resolución 0839 de 2025, y con decisión de aprobar este acto administrativo.

Que, en mérito de lo expuesto este despacho,

RESUELVE

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto. La presente resolución tiene por objeto actualizar la Política de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la operación de los servicios del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, con el fin de promover lineamientos para el manejo, uso y protección de la información de la Entidad.

Artículo 2. Ámbito de aplicación. Serán sujetos obligados de la presente resolución, todos los niveles funcionales, organizacionales y dependencias de la Entidad, así como todos los funcionarios, contratistas, pasantes, profesionales en entrenamiento, investigadores visitantes, colaboradores, proveedores y demás personas o terceros que compartan, utilicen, recolecten, procesen, intercambien o consulten su información bien sea permanente, temporal o transitoria, al igual que a las entidades de control y demás

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

entidades relacionadas que accedan, ya sea de manera interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, esta política aplica a toda la información creada, inventada, desarrollada, procesada o utilizada por la Entidad sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Artículo 3. Política General de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS. Los sujetos descritos en el ámbito de aplicación deberán preservar y administrar la integridad, confidencialidad, disponibilidad, privacidad, legalidad y confiablidad de la información digital y física, que se produce en el marco de la operación de sus procesos misionales y/o contractuales, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo la prestación ininterrumpida de los servicios científicos, técnicos y de salud pública del INS, con calidad, transparencia, responsabilidad y respetando las disposiciones vigentes en materia de tratamiento de datos personales, en beneficio de la ciudadanía, el sistema de salud y las instituciones que conforman el Sistema Nacional de Ciencia, Tecnología e innovación.

Artículo 4. Objetivos de la Política General. La Política de Seguridad y Privacidad de la Información y Seguridad Digital, tendrá los siguientes objetivos:

- Establecer mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, imparcialidad, disponibilidad, privacidad, legalidad y confiabilidad de la información del INS.
- Mitigar el impacto de los incidentes de seguridad y privacidad de la información y seguridad digital en el INS.
- Gestionar los riesgos de seguridad y privacidad de la información y de seguridad digital.
- Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto desempeño del sistema de gestión de seguridad y privacidad de la información.
- Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
- Definir y operar la continuidad de la operación de los servicios tecnológicos del INS.
- Garantizar el acceso libre a la ciudadanía de la información pública en poder de la entidad, con el fin de garantizar el cumplimiento del derecho de acceso a la información pública nacional.

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

CAPÍTULO II
POLÍTICAS GENERALES ORGANIZACIONALES

Artículo 5. Política de seguridad de la información en la gestión de proyectos. Esta política busca que desde la gestión de los proyectos se traten los lineamientos frente a la seguridad y privacidad de la información independientemente del tipo de proyecto. La Oficina Asesora de Planeación y el personal de apoyo, deberá incluir los requerimientos y consideraciones en materia de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, en la metodología de gestión de proyectos de la Entidad, garantizando que se implementen en las fases iniciales de los proyectos, en el mismo sentido, la Oficina Asesora de Control Interno y el personal de apoyo, podrá implementar seguimientos, monitoreos, planes de auditoría interna u otros mecanismos de control, para la revisión del cumplimiento e implementación de la política, dependiendo de las necesidades de la Entidad.

Artículo 6. Política de gestión de activos. La OTIC y la Secretaría General, en su marco de competencias, articularán el diseño y la adopción de los lineamientos específicos para la identificación, clasificación, valoración, rotulado (etiquetado) y buen uso de los activos de información, con el objetivo de garantizar su protección. Dichos lineamientos se construirán e impartirán teniendo en cuenta los siguientes criterios:

- **Inventario de Activos:** Los activos del Instituto deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. La OTIC y el Grupo de Gestión Documental, diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminado por procesos y dependencia, tipo, nivel de criticidad, duración de la confidencialidad y reserva de la información, clasificación, ubicación, responsable, custodio, y demás atributos que la entidad defina.
- **Protección:** Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros establecidos.
- **Archivos de Gestión:** El Grupo de Gestión Documental deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental y Tablas de Control de Acceso, con el fin de proteger y conservar la confidencialidad, integridad, imparcialidad y disponibilidad de la información física del Instituto.
- **Sistema de gestión de documento electrónico de archivo- SGDEA:** El Grupo de Gestión Documental con el apoyo de la OTIC, deberán implementar un sistema de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información. Adicionalmente, para la emisión, recepción y gestión

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

de comunicaciones oficiales, a través de los diversos canales electrónicos y físico, deberá asegurar un adecuado tratamiento archivístico.

- **Clasificación de la Información:** La OTIC en conjunto con el Grupo de Gestión Documental deberán establecer lineamientos para la clasificación y rotulado (etiquetado) de la información del Instituto, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014 (ley de transparencia y acceso a la información), esta última reglamentada por el Título 1 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 y en el Título 3 de la Parte 8 del Libro 2 del Decreto 1080 de 2015 y demás normativa que reglamente la clasificación de información de las entidades públicas del país. Así mismo, la OTIC implementará una herramienta informática que permita rotular (etiquetar) la información digital.
- **Firma de documentos:** Las firmas de documentos que produzca el Instituto será válida en cualquiera de los siguientes métodos, garantizando la confiabilidad, integridad, autenticidad y disponibilidad de la información de los documentos expedidos por los servidores públicos y contratistas en el marco de sus funciones y competencias, así:

  - En físico con firma autógrafa mecánica.
  - Con firma digital de persona natural asignadas por la OTIC según lo dispuesto por la Ley 527 de 1999 o la norma que la modifique, adicione o sustituya.
  - Con firma electrónica, de acuerdo con lo dispuesto en los Decretos 2364 de 2012 y 1287 de 2020, o la norma que los modifique, adicionen o sustituyan, para lo cual el Instituto deberá adquirir o implementar un aplicativo que contenga como mínimo lo siguiente:
    - Control seguro de acceso y uso al aplicativo, sincronizado con el directorio activo, garantizando que solo personal vinculado pueda hacer uso del mecanismo de firma electrónica,
    - Múltiples controles para la autenticación y firma del documento electrónico, garantizando que el firmante es quien dice ser.
    - El sistema debe solicitar la firma digitalizada o escaneada y quedar estampada en el documento junto con el nombre completo, cargo, correo electrónico institucional del servidor o contratista que firma.
    - Identificador único provisto por el sistema que permita la verificación de la veracidad del documento.
    - Fecha de creación y finalización de la firma provisto por el servidor y sincronizado con la hora legal colombiana.
    - Estado del trámite de firma.
    - Firma digital del funcionario quien ejerce la representación del Instituto, según sea el caso.
    - En ningún caso se debe utilizar firmas facsímil, salvo en aquellos que se autorice por resolución expedida por el director del Instituto, indicando para que fin y porqué medios podrá ser utilizada.

Parágrafo. Durante el proceso de transición e implementación de lo anterior, el proceso de firma de los documentos expedidos para el desarrollo misional y de apoyo de la

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

Entidad, se seguirá realizando de acuerdo con lo definido en artículo 7 de la Ley 527 de 1999, reglamentado por el Decreto 2364 de 2012.

Artículo 7. Política de control de acceso. De conformidad con lo establecido con la Guía Técnica Colombiana GTC-ISO/IEC 27002:2022, los propietarios de los activos de información, teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías e infraestructura física (instalaciones y oficinas), todo esto con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado y así propender por salvaguardar la integridad, disponibilidad, confidencialidad y privacidad de la información del Instituto.

Artículo 8. Política de seguridad para la relación con proveedores. Esta política busca establecer las condiciones para la prestación de los servicios, responsabilidades y controles que ayuden a proteger la información involucrada en las relaciones entre el Instituto con terceros, frente a interceptaciones, copia, modificación, divulgación, destrucción no autorizada y los riesgos asociados a la adquisición de productos y servicios de seguridad digital que puedan afectar los principios de integridad, imparcialidad, disponibilidad, privacidad y confidencialidad de la información. Aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica del Instituto.
El Grupo de Gestión Contractual, establecerá y documentará, las disposiciones necesarias para asegurar que la información que se genere, trate, custodie, procese, comparta, utilice, recolecte, intercambie o a la que se tenga acceso con ocasión de un contrato, se utilice dentro del marco de la seguridad y privacidad de la información por parte de los proveedores. En el mismo sentido y a través del seguimiento a la ejecución, se garantizará que los supervisores de los contratos, convenios o acuerdos sean los responsables de aplicar las políticas y procedimientos de seguridad y privacidad de la información durante la ejecución de los contratos, estos lineamientos deberán ser comunicados a los proveedores a través de los canales dispuestos por el Instituto.

Parágrafo. Tratándose de relaciones contractuales del Instituto, estas disposiciones deberán ser incorporadas en los términos, cláusulas, minutas o acuerdos con los que se relacionen estos, a efectos de garantizar su implementación.

Artículo 9. Política de gestión de incidentes de seguridad y privacidad de la información y seguridad digital. Esta política busca gestionar adecuadamente todos los incidentes de seguridad y privacidad de la información y seguridad digital reportados en la Entidad, dando cumplimiento a los procedimientos establecidos para el efecto. Aplica para todos los servidores públicos, aplicaciones, y terceros del Instituto que detecten un evento o incidente de seguridad y privacidad de la información y seguridad digital, el cual deben reportar, adecuadamente, de acuerdo con los procedimientos establecidos. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, promoverá entre los empleados públicos, contratistas y terceros, el reporte y

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

seguimiento de incidentes relacionados con la seguridad y privacidad de la información y seguridad digital, y sus medios. Así mismo, asignará responsables para el tratamiento de estos, quienes investigarán y solucionarán los incidentes reportados, de acuerdo con su criticidad.
El Oficial de Seguridad y Privacidad de la Información informará a la Dirección General del Instituto, los incidentes de seguridad, para que éste en el marco de sus competencias, reporte e instaure las denuncias ante las autoridades pertinentes, tales como, defensa nacional, policía, fiscalía y de control. La Dirección General o quien esta delegue, será el único canal de comunicación autorizado para hacer pronunciamientos oficiales ante las entidades externas, medios de comunicación o la ciudadanía.

Artículo 10. Política de la continuidad de la operación de los servicios. Esta política busca asegurar que todos los aspectos relacionados con la seguridad de la información se incluyan en los planes de continuidad de la operación de la Entidad y así proteger la información. Esta política aplica para la definición del plan de continuidad de operación de servicios y la recuperación en caso de desastres, en las cuales se deben incluir los requisitos de seguridad y privacidad de la información. El Instituto dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos.
El Oficial de Seguridad y Privacidad de la Información y la OTIC liderarán conjuntamente la elaboración del Análisis de Impacto del Negocio (BIA) y del Plan de Recuperación ante Desastres (DRP) tecnológicos.

Artículo 11. Política de cumplimiento. Esta política busca evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad y privacidad de la información, y de cualquier requisito de esta índole en la Entidad y asegurar que se revisen y actualicen periódicamente, como mínimo una vez al año o cuando se presente una actualización en la normatividad que afecte la seguridad y privacidad de la información. Esta será aplicada por todas las dependencias del Instituto.

El Oficial de Seguridad y Privacidad de la Información con apoyo de la Oficina Asesora Jurídica y su personal de apoyo, y el Asesor de Planeación, velarán por la identificación, documentación, cumplimiento y asesoría de los requisitos legales enmarcados en la seguridad y privacidad de la información y seguridad digital, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a la propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, para lo cual dispondrá de procedimientos y una matriz de requisitos legales para su control y seguimiento.

Artículo 12. Política de privacidad. El Instituto deberá disponer, a través del Oficial de protección de datos personales o quien haga sus veces de los controles necesarios para la protección de la información de los empleados públicos, contratistas y partes

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

interesadas externas, en los términos de la Ley 1581 de 2012 y sus decretos reglamentarios, así como la política de tratamiento de datos personales de la Entidad.

Parágrafo 1. El Oficial de protección de datos personales o quien haga sus veces delegado en el Instituto, en conjunto con el Grupo de Gestión Contractual, diseñarán un formato de autorización y uso de datos personales, así como de su tratamiento, que deberá adoptar Entidad, en lo que respecta al uso de datos semiprivados, privados, sensibles, de niños, niñas y adolescentes; dicho formato debe ser claro y detallado en lo referente a la recolección de los datos personales; así mismo, deberá ser firmado por todos los empleados públicos y contratistas en el momento de su vinculación al INS.

Parágrafo 2. El Oficial de Seguridad y Privacidad de la Información en conjunto con la Oficina Asesora de Comunicaciones, diseñarán y actualizarán los formatos de autorización, por parte de los ciudadanos, de la captación y uso de imágenes, videos o cualquier medio audiovisual, de conformidad con lo dispuesto en las normas vigentes sobre protección de datos personales, en especial la Ley 1581 de 2012 y sus normas reglamentarias y el Decreto 1074 de 2015 o la norma que lo modifique, adicione o sustituya, así como su autorización libre, expresa e inequívoca a el Instituto o a quien este autorice o encargue, para el uso del recurso audiovisual en el marco del cumplimiento de su misión.
Los formatos deberán prever la opción en caso de que el ciudadano sea menor de edad y se deberá establecer lineamientos para el caso en que el ciudadano no autorice dicho tratamiento.

Parágrafo 3. La toma de material audiovisual a los ciudadanos mayores o menores de edad sólo se podrá realizar por los empleados públicos o contratistas avalados por la Oficina Asesora de Comunicaciones y en cumplimiento de las funciones de acompañamiento del Instituto o donde éste fuere invitado de manera oficial. Los datos que se recolecten solo podrán ser tratados para el cumplimiento de la finalidad para la cual se ha dispuesto el tratamiento.

CAPÍTULO III
POLÍTICAS GENERALES DEL RECURSO HUMANO

Artículo 13. Política de seguridad y privacidad en el recurso humano. Esta política asegura que tanto los funcionarios como los contratistas comprendan las responsabilidades en los roles que ejercen en la Entidad y tomen conciencia respecto a la implementación de los lineamientos de seguridad y privacidad con el fin de preservar la disponibilidad, integridad, privacidad y confidencialidad de la información del Instituto. Para el efecto, el Grupo de Gestión del Talento Humano y el Grupo de Gestión Contractual con el apoyo del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces deberán:

- Desplegar esfuerzos para generar conciencia y apropiación en los empleados públicos de la entidad y contratistas, sobre sus responsabilidades con el fin de reducir

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

los riesgos, el mal uso de las instalaciones y recursos tecnológicos y así asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información.

- Incluir en las minutas de los contratos y convenios, cualquiera que sea su naturaleza o modalidad, cláusulas y obligaciones, las cuales deberán ser divulgadas a través de los supervisores de los contratos, a proveedores y aquellas personas o terceros que, debido al cumplimiento de sus funciones, obligaciones y las de la entidad, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.
- Fomentar la participación de los empleados públicos de la entidad en las convocatorias para el fortalecimiento de capacidades en seguridad digital realizadas por el Gobierno Nacional u organismos internacionales.

Parágrafo 1. Como parte de sus términos y condiciones iniciales de trabajo de todos los empleados públicos, sin importar su nivel jerárquico, o los contratistas de la entidad, según el caso, firmarán un acuerdo o compromiso de confidencialidad y no divulgación, que será elaborado por la Oficina Asesora Jurídica con el apoyo del Oficial de Seguridad y Privacidad de la Información, según el tipo de vinculación, en lo que respecta a la información del Instituto. Dicho documento original será conservado y archivado en la historia laboral de los empleados públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

Parágrafo 2. En el caso de persona jurídica proveedora de servicios para la entidad, en la carpeta del contrato deberá reposar el acuerdo o compromiso de confidencialidad y no divulgación debidamente suscrita por el representante legal.

CAPÍTULO IV
POLÍTICAS GENERALES PARA LA PROTECCIÓN FÍSICA

Artículo 14. Política de seguridad física y del entorno. El Instituto, a través de El Grupo de Gestión Administrativa y el Oficial de Seguridad y Privacidad de la Información, debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas, áreas destinadas al procesamiento o almacenamiento de información clasificada o reservada, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, con el fin de mitigar los riesgos, amenazas externas, ambientales y evitar afectación a la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad.

Parágrafo 1. El Grupo de Gestión Administrativa, en conjunto con el Oficial de protección de datos personales o quien haga sus veces, deberán garantizar la protección de los datos semiprivados, privados o sensible recolectados en el área de acceso a las instalaciones de la entidad de los empleados públicos, contratistas y visitantes, en lo que refiere el artículo 12 de la presente resolución y establecer mecanismos alternativos para quienes no autorizan el tratamiento de sus datos.

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

Parágrafo 2. Todos los empleados públicos, contratistas y visitantes que se encuentren en las instalaciones físicas del Instituto deben estar debidamente identificados, con un carné, documento o distintivo que acredite su tipo de vinculación, en caso del carné, este debe portarse en un lugar visible.

Parágrafo 3. Los visitantes que se encuentren en las instalaciones del Instituto siempre deben permanecer acompañados por un empleado público o contratista de la entidad debidamente identificado.

Parágrafo 4. El personal de empresas, cooperativas o entidades que desempeñe funciones de forma permanente en las instalaciones de la entidad, deben estar identificados con carné o chalecos o distintivos de la empresa o entidad y tener vinculación a una Administradora de Riesgos Laborales - ARL.

CAPÍTULO V
POLÍTICAS GENERALES DE TECNOLOGÍA

Artículo 15. Política de seguridad de las operaciones. Esta política busca asegurar la operación y administración de los recursos tecnológicos que soportan la operación de la entidad. Para el efecto la OTIC, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad, disponibilidad y privacidad de la información e implantará una mesa de control de cambios, reglamentado mediante unos lineamientos, para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de producción sean controlados y debidamente autorizados, así mismo implementará mecanismos para controlar la información en los ambientes de desarrollo y prueba, en los casos que aplique.

De igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la entidad, al igual que desarrollará mecanismos de contingencias y recuperación ante desastres con el fin de propender por la disponibilidad de los servicios de TI en el marco de la operación de la entidad.

La OTIC deberá realizar y mantener copias de seguridad de la información de la entidad en medio digital, con el objetivo de recuperarla en caso de cualquier tipo de falla. Estas copias se realizarán, de acuerdo con el esquema definido previamente en un procedimiento que enmarque la gestión de las copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la entidad.

El diseño de este procedimiento se hará bajo la OTIC, con el apoyo de los líderes de proceso y deberá estar alineado con la gestión documental de la entidad, con el fin de

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

determinar la información a respaldar, la periodicidad, los tiempos de retención, recuperación, restauración y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

Artículo 16. Política de criptografía. La OTIC dispondrá de herramientas que permitan el cifrado de la información clasificada y reservada para proteger su confidencialidad, integridad, disponibilidad y privacidad.

Artículo 17. Política de seguridad de las comunicaciones. Esta política busca fortalecer la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de la entidad, así como los controles utilizados para proteger la información en la transferencia de información. Para el efecto la OTIC establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios tecnológicos que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la entidad.

La OTIC establecerá mecanismos estratégicos para que el intercambio de información con las partes interesadas internas o externas, se realice asegurando su integridad. En el evento que los acuerdos de intercambio de información requieran del desarrollo de servicio web (web service) o de cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos definidos en la entidad.

Artículo 18. Política de seguridad para la adquisición, desarrollo y mantenimiento de sistemas. Esta política busca asegurar que la seguridad digital sea una parte integral de los sistemas de información de la Entidad durante todo el ciclo de vida y aplica a todos los sistemas de información, incluyendo los sistemas de información que prestan servicios sobre redes públicas. La OTIC velará porque los desarrollos internos y externos de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información de la entidad, para lo cual, establecerá una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información.

En el marco del Plan Estratégico de Tecnologías de la Información (PETI), la OTIC es la única dependencia con la capacidad de adquirir, conforme con su ficha de inversión, desarrollar e implementar soluciones tecnológicas para el Instituto, así como de avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme a los requerimientos de las dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la entidad.

En consecuencia, cualquier software que opere en la entidad deberá contar con la autorización de la OTIC y deberá reportarse y entregarse cumpliendo con los lineamientos técnicos y presupuestales de dicha oficina, con el fin de salvaguardar la

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro.

Parágrafo. En caso de que alguna dependencia adquiera, desarrolle o realice mantenimientos a sistemas de información dentro del desarrollo misional u operacional de la entidad, deberá cumplir con lo establecido en la presente política.

Artículo 19. Política de seguridad digital. Esta política busca establecer un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior de la entidad por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido por el Instituto, buscando preservar la confidencialidad, integridad, privacidad y disponibilidad de la información. Aplica a todos los empleados públicos o contratistas que hagan uso de los recursos tecnológicos de la entidad, que tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y, por ende, el cumplimento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

1. **Del uso del correo electrónico.** El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los empleados públicos y contratistas de la entidad, cuyo uso se facilitará en los siguientes términos:

   a. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por la OTIC, que cuenta con el dominio @ins.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
   b. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la entidad.
   c. En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita.
   d. Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones), o la que la modifique, adicione o sustituya, la cual establece la validez de los mensajes de datos.

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

e. La OTIC implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada, de conformidad con la Ley 1712 de 2014 o la que la modifique, adicione o sustituya.

f. Se prohíbe el envío de correos masivos (más de 30 destinatarios) internos o externos, con excepción de los enviados desde cuentas genéricas por la Dirección, Oficina Asesora de Comunicaciones, Grupo de Gestión del Talento Humano, Oficina Asesora de Planeación, así como de la OTIC solamente en caso de ventana de mantenimientos de los servicios de tecnología de la información. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.

g. Todo mensaje de correo electrónico enviado por la entidad mediante plataformas externas deberá hacerse con una cuenta del Instituto y utilizando el dominio @ins.gov.co, con el fin de que no sean catalogados como spam o suplantación de correo.

h. Para apoyar la gestión de correo electrónico de directivos, asesores y jefes, el titular debe solicitar a la mesa de servicios la delegación del buzón correspondiente, relacionando los colaboradores que podrán escribir o responder en nombre del titular, con el fin de mitigar la suplantación.

i. Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la OTIC a través de la Mesa de Servicios o canal disusto para su reporte como evento de seguridad y privacidad de la información o seguridad digital, según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o explícitas referencias no relacionadas con la misión de la entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.

j. La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la entidad.

k. Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones.

l. Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada del Instituto a otras entidades o ciudadanos sin la debida autorización de la Dirección General, de la Oficina Asesora de Comunicaciones y de la Oficina Asesora de Planeación, previa revisión del Asesor/a de Comunicaciones en caso de comunicados y del Asesor/a de Planeación en caso de cifras oficiales.

m. El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la ley.

n. El correo electrónico institucional en sus mensajes debe incorporar un aparte con contenido de confidencialidad y la respectiva firma de correo, que será diseñado por la OTIC con el apoyo del equipo de Comunicación, dicha sentencia y firma debe reflejarse en todos los buzones con dominio @ins.gov.co.

o. Está expresamente prohibido distribuir, copiar o reenviar información del Instituto a través de correos personales o sitios web diferentes a los autorizados en el

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

marco de las funciones u obligaciones contractuales, so pena de sanciones legales a que haya lugar.

p. Cuando un empleado público o contratista cesa en sus funciones o culmina la ejecución de contrato con la entidad, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa de la Dirección General, por orden judicial o por solicitud del Asesor/a de Control Interno como parte de un proceso de investigación.

q. La entidad se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus empleados públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados en la misma, previa solicitud expresa del nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, Director general; a La OTIC. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los funcionarios y contratistas que el Instituto realiza el referido monitoreo.

r. En el caso de hacer envíos de comunicaciones masivas con correos personales, evitar que estos queden expuestos y de acceso no autorizados. Por ejemplo, hacer uso de las copias ocultas (CCO).

2. **Del uso de Internet:** La OTIC, en conjunto con el Oficial de Seguridad y Privacidad de la Información, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los colaboradores las siguientes, entre otras:

   a. Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol, funciones u obligaciones que desempeña en el Instituto y para las cuales esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.

   b. Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.

   c. Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación de la entidad.

   d. Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.

   e. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

   f. La entidad se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la entidad.

3. **Del uso de los recursos tecnológicos:** Los recursos tecnológicos de la Entidad son herramientas de apoyo a las labores, responsabilidades y obligaciones de los

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

empleados públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

a. Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del empleado público o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la OTIC, salvo que medie solicitud formal de la Dirección General, jefes de oficina y coordinadores, a través de la Mesa de Servicios.
b. Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la OTIC.
c. En caso de que el empleado público o contratista deba hacer uso de equipos ajenos a la entidad, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red de la entidad una vez esté avalado por la OTIC.
d. Los empleados públicos y contratistas deberán hacer uso de los repositorios autorizados, y mantener la información en estos, con el fin de entregarla a la entidad al finalizar la vinculación o terminación contractual.
e. Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional o que atenten contra la propiedad intelectual de titularidad de terceros.
f. Los empleados públicos y contratistas deberán utilizar las herramientas tecnológicas que proporcione la OTIC para gestionar la información digital del Instituto.
g. No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y, por ende, a la pérdida de la integridad de ésta.
h. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente por el Grupo de Gestión Administrativa.
i. Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son las designadas para tal labor por la OTIC.
j. La OTIC realizará control y monitoreo sobre los dispositivos de almacenamiento externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información clasificada y reservada.
k. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la OTIC, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.
l. La pérdida o daño de elementos o recursos tecnológicos suministrados por el INS, o de alguno de sus componentes, deberá ser informada de inmediato a la OTIC por el empleado público o contratista a quien se le hubiere asignado; en caso de

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

que el equipo de cómputo sea suministrado por la Entidad, deberá reportarse al Grupo de Gestión Administrativa siguiendo los procedimientos establecidos para este tipo de siniestros, sin perjuicio de las acciones penales y disciplinarias que requiera adelantar según sea el caso.

m. La pérdida de información deberá ser informada con detalle a la OTIC, a través de la Mesa de Servicios, como incidente de seguridad y privacidad de la información.

n. Todo incidente de seguridad y privacidad que comprometa la confidencialidad, integridad, disponibilidad y privacidad de la información física o digital deberá ser reportado a la mayor brevedad a la OTIC, a través de la mesa de servicios, siguiendo el procedimiento establecido.

o. La OTIC es la única dependencia autorizada para la administración del software del Instituto, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

p. Todo acceso a la red de la Entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por La OTIC.

q. La conexión a la red wifi institucional para empleados públicos y contratistas deberá ser administrada desde la OTIC mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo.

r. La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por la OTIC, las contraseñas deberán cambiar los lunes de cada semana.

s. La red Wifi para empleados públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por la entidad.

t. Los equipos en la medida de lo posible deben quedar apagados cada vez que el empleado público o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la entidad, siempre y cuando no vaya a realizar actividades vía remota.

u. Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad debe acogerse a las políticas de "Trae tu propio dispositivo".

v. Las herramientas corporativas instaladas en los dispositivos móviles personales serán gestionadas por la OTIC con el fin de proteger la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad, garantizando el cumplimiento del artículo 12 de la presente resolución.

4. **Del uso de los sistemas o herramientas de información:** Todos los empleados públicos y contratistas de la entidad son responsables de la protección de la información a la que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

a. Las credenciales de acceso a la red y a los recursos informáticos (usuario y clave) son de carácter estrictamente personal e intransferible; los empleados públicos y contratistas no deben revelarlas a personal interno o externo, ni utilizar claves ajenas.

b. Todo empleado público y contratista deberá realizar el cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos, teniendo

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

en cuenta los lineamientos establecidos para la periodicidad de cambio y robustez de estas.

c. Todo empleado público y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
d. En ausencia del empleado público por algún tipo de novedad (vacaciones, licencias o bajo una suspensión parcial de sus funciones) o ausencia del contratista, el acceso a la cuenta de usuario le será bloqueada con una solicitud a la OTIC a través de la Mesa de Servicios, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. El Grupo de Gestión del Talento Humano debe reportar de inmediato, cualquier tipo de novedad de los empleados públicos, a su vez los supervisores de contrato deben reportar oportunamente todas las novedades del contratista.
e. Cuando un empleado público o contratista cesa sus funciones o culmina la ejecución del contrato con el Instituto, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información que estos ostenten será almacenada en los repositorios de la entidad.
f. Cuando un empleado público o contratista cesa sus funciones o culmina la ejecución del contrato con el Instituto, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.
g. Cuando un empleado público o contratista cesa sus funciones o culmina la ejecución del contrato con el Instituto deberá tramitar el paz y salvo, de acuerdo con el procedimiento establecido por la entidad.
h. Todos los empleados públicos y contratistas de la entidad deben dar estricto cumplimiento a lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

Artículo 20. Política para el uso responsable de la inteligencia artificial. El Instituto Nacional de Salud - INS promoverá el uso responsable, ético, transparente y seguro de tecnologías basadas en Inteligencia Artificial (IA) en el desarrollo de sus funciones misionales, científicas, técnicas y administrativas exclusivamente como fuente de consulta y no como gestor de la actividad misional. Esta política busca garantizar que la implementación de soluciones de IA respete los derechos fundamentales, la protección de datos personales, la seguridad de la información y los principios de equidad, no discriminación y explicabilidad citando las fuentes de información.

Parágrafo 1. Toda iniciativa, proyecto o sistema que utilice algoritmos de IA deberá ser evaluado previamente por la Oficina de Tecnologías de la Información y las Comunicaciones, en coordinación con la Oficina Asesora Jurídica y las áreas funcionales involucradas, para verificar su alineación con los principios institucionales, la normativa vigente y los estándares internacionales en ética digital.

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

Parágrafo 2. El INS deberá asegurar que los sistemas de IA utilizados o desarrollados por la entidad cuenten con mecanismos de trazabilidad, supervisión humana, gestión de riesgos y documentación técnica que permita explicar sus decisiones y resultados.

Parágrafo 3. Se prohíbe el uso de herramientas de IA que comprometan la confidencialidad, integridad o disponibilidad de la información institucional, que generen sesgos injustificados, o que no cuenten con licenciamiento, validación técnica o respaldo legal.

Parágrafo 4. La capacitación del talento humano en el uso ético y seguro de la IA será promovida como parte de la cultura institucional de innovación y transformación digital.

CAPÍTULO VI
DISPOSICIONES FINALES

Artículo 21. Lineamientos de las políticas de seguridad de la información. El Instituto, deberá desarrollar de manera detallada y clara estas políticas en la Declaración de Aplicabilidad y el Manual de Política de Seguridad y Privacidad de la Información y Seguridad Digital, que serán publicadas de acuerdo con el Sistema Integrado de Gestión - SIG.

Artículo 22. Designación del Oficial de Seguridad y privacidad de la Información. El Director(a) General del INS designará el funcionario y asignará las funciones que ejercerá el Oficial de Seguridad y Privacidad de la Información, en los términos definidos en la presente resolución.

Artículo 23. Revisión. La Política de Seguridad y Privacidad de la Información y Seguridad Digital, será revisada anualmente y se harán ajustes antes, si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz.

Artículo 24. Seguimiento. El cumplimiento de las Políticas de Seguridad y Privacidad de la Información y seguridad Digital serán verificadas a través de la Oficina Asesora de Control Interno por medio de seguimientos, monitoreos u otros mecanismos de control.

Artículo 25. Transición. Las disposiciones previstas en la presente resolución se implementarán de manera gradual de acuerdo con el plan de trabajo presentado por la OTIC al Comité Institucional de Gestión y Desempeño.

Artículo 26. Vigencia. La presente Resolución rige a partir de la fecha de su publicación y deroga la Resolución 0839 de 2025 y demás normas que le sean contrarias.

"Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025"

COMUNÍQUESE Y CÚMPLASE

04 DIC 2025

Dada en Bogotá D.C., a los días del mes de diciembre de 2025

DIANA MARCELA PAVA GARZÓN
Directora General

Revisó: Carlos Andrés López Fernández – Jefe de OTIC
Ingrit Lineth Vásquez Cely – Jefe – Oficina Asesora Jurídica (e)
Giovanni Agudelo González - Contratista - Oficina Asesora Jurídica
Javier Ricardo Bohórquez Gelvez – Jefe de Oficina Asesora de Planeación
Henry Alfredo Cruz Rincón – Asesor Jurídico de la Dirección General
Elaboró: Sergio Andrés Ramos Pahuana – Contratista OTIC