1. OBJETIVO

Establecer los lineamientos para preservar la seguridad de la información y la protección de los datos personales, bajo condiciones de uso confiable en el entorno digital y físico, mediante una adecuada gestión de riesgos que garantice la confidencialidad, integridad y disponibilidad de la información y los datos tratados, así como de los servicios que el Invima presta al ciudadano. Lo anterior, en cumplimiento de los requisitos del Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Seguridad Digital y Gobierno Digital, y demás disposiciones legales que rigen las funciones del Instituto, buscando permanentemente la satisfacción de las necesidades de las partes interesadas.

2. ALCANCE

La presente Política de Seguridad Digital aplica a la totalidad de las dependencias del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, así como a todos sus procesos institucionales. Igualmente, es de obligatorio cumplimiento para los servidores públicos, contratistas y demás colaboradores de la Entidad, así como para terceros que, en el desarrollo de sus actividades, mantengan cualquier tipo de relación o vínculo con el Instituto y tengan acceso a sus sistemas de información, recursos tecnológicos o activos digitales.

3. MARCO NORMATIVO Y LEGAL

- **Constitución Política de Colombia de 1991** *“Articulo 15”, “Articulo 20”, “Articulo 74” y “Articulo 209”.*
- **Ley 23 de 1982** *“Sobre derechos de autor”*
- **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.”*
- **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.”*
- **Ley 1474 de 2011** *“Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública."*
- **Ley 1437 de 2011** *“Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.”*
- **Ley 1581 de 2012** *“Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Sentencia C-748 de 2011. Decreto 255 de 2022. Por la cual se dictan disposiciones generales para la protección de datos personales.”*
- **Ley 1712 de 2014** *“Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.”*
- **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 1083 de 2015** *Sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, (“11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital)*
- **Ley 1755 de 2015** *“Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.”*
- **Resolución 500 de 2021** *“Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.”*
- **Decreto 338 de 2022** *“Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de*

establecer los 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."

- **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, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones."*

OTROS DOCUMENTOS DE REFERENCIA

- Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG).
- Modelo Estándar de Control Interno (MECI).
- Mapa de Riesgos de Corrupción y Planes Anticorrupción de la entidad.
- Políticas institucionales.

4. POLITICA

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, está comprometido con proteger y promover la salud de la población, mediante la gestión del riesgo, asociada al consumo y uso de alimentos, medicamentos, dispositivos médicos y otros productos objeto de vigilancia sanitaria.
Para procurar la prestación óptima, continua y segura de sus servicios, así como el cumplimiento de sus procesos de vigilancia y control sanitario, el Instituto asegura la protección de la información y de los datos personales mediante la implementación de un proceso permanente de gestión de riesgos. Este proceso permite identificar, evaluar y tratar los riesgos, estableciendo los controles necesarios para que los niveles de exposición se mantengan dentro de los límites definidos por la Alta Dirección. Asimismo, el Instituto fortalece las competencias de su talento humano en buenas prácticas de seguridad, promueve la mejora continua del sistema de gestión y optimiza el uso de los recursos disponibles, con el fin de satisfacer los requisitos de seguridad de las partes interesadas y dar cumplimiento a las disposiciones normativas aplicables al Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima.
Para el cumplimiento de lo anteriormente mencionado se establecen los siguientes principios

- Asegurar el uso de la información y los datos personales del instituto y que aplique bajo las medidas de seguridad exigidas por el estado para garantizar el derecho de habeas datas de los ciudadanos y prevenir perdidas de confidencialidad, integridad y disponibilidad sobre los mismos.
- Preservar la confidencialidad de la información del instituto dentro del marco que regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
- Adoptar todas las medidas de seguridad de la información tanto administrativas como tecnológicas que estén a su alcance para preservar la confidencialidad, integridad, disponibilidad y autenticidad de la información que reposa dentro de los activos de información que está bajo responsabilidad de instituto, de sus servidores públicos, contratistas, proveedores, operadores, terceros o de todas aquellas personas naturales o jurídicas que tengan algún tipo de relación con la entidad y que, de conformidad con la normativa vigente, sean objeto de tratamiento.
- Implementar acciones de mejora continua que permitan identificar, reportar y controlar oportunamente eventos que pueden constituir amenazas o vulnerabilidades potenciales o reales sobre los activos de información institucionales.

5. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección del Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

6. ROLES Y RESPONSABILIDADES

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos – Invima, define los roles y responsabilidades para la implementación del subsistema de gestión de seguridad de la información considerando los lineamientos del sistema de gestión integrado, el cumplimiento de los lineamientos de seguridad descritos en la política de seguridad institucional, así como las obligaciones descritas en manuales, procedimientos, formatos y demás documentación del sistema de gestión integrado del Instituto.

Dependencia	Responsabilidades frente a la seguridad de la información
Dirección general	• La Alta dirección demuestra su liderazgo y compromiso frente a la gestión de la seguridad de la información con el establecimiento de la política del Sistema de Gestión de Seguridad de la Información y sus objetivos, velando porque estos contribuyan al logro de la misión y visión de la Entidad. • Apoyar la integración del subsistema de gestión de seguridad de la información con los procesos de la entidad, aprueba el uso recursos económicos y de personal institucionales que contribuyan al mejoramiento de un entorno digital seguro para los activos de información institucionales • Impulsar a todos los servidores públicos y contratistas para que conozcan y apliquen las políticas y procedimientos en materia de seguridad de la información • Realizar el seguimiento en intervalos planificados al sistema integrado de gestión institucional y a la implementación del subsistema de gestión de seguridad de la información para evaluar su contribución al logro de los objetivos de la seguridad de la información declarados en la política. • Fomentar, apoyar y velar por la formación de Auditores Internos en materia de seguridad de la información, que permitan una evaluación independiente de los resultados de la gestión de la seguridad de la información • Se Asegura, que las responsabilidades para los roles de la Seguridad de la información se asignen y comuniquen oportunamente.
Comité institucional de desarrollo y desempeño	De conformidad con lo establecido en el DECRETO 1499 DE 2017 (septiembre 11) *"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015" las responsabilidades del comité institucional de gestión y desempeño en materia de seguridad de la información cubren*: *ARTÍCULO 2.2.22.3.8. Comités Institucionales de Gestión y Desempeño.* *2. Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión - MIPG.* *6. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.* Para lograr el cumplimiento de sus responsabilidades en materia de seguridad digital y de la información, el comité institucional de gestión y desempeño: • Coordinar y apoyar la implementación del Modelo de Seguridad y privacidad de la Información en Invima. • Revisar y aprobar las actualizaciones y los nuevos lineamientos en materia de seguridad de la información. • Presentar a la alta dirección los requerimientos presupuestales para la implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información en Invima.

- Evaluar y aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información establecido en el DECRETO 612 DE 2018 (Abril 4) Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. Articulo "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción.
- Velar porque el Plan Institucional de Capacitación incluya acciones de sensibilización y toma de conciencia en materia de seguridad de la información.
- Apoyar a la Alta dirección en la realización de las revisiones anuales periódicas del sistema integrado de gestión institucional que incluyen al subsistema integrado de gestión y que mediate sus resultados facilitan el reporte del FURAG (Formulario Único de Reporte de Avances de la Gestión) del Departamento administrativo de la Función Pública.

Servidores públicos, contratistas, colaboradores y/o, terceros .

De conformidad con Ley 1952 de 2019 "por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario. son responsabilidades en materia de seguridad de la información de todos los servidores del INVIMA:
ARTÍCULO 38. Deberes. Son deberes de todo servidor público:
5. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.
6. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.
ARTÍCULO 39. Prohibiciones. A todo servidor público le está prohibido:
18. Dar lugar al acceso o exhibir expedientes, documentos o archivos a personas no autorizadas.
Para lograr el cumplimiento de sus obligaciones en materia de seguridad de la información, todos los servidores, contratistas y demás colaboradores de la Entidad, así como para terceros que, en el desarrollo de sus actividades, mantengan cualquier tipo de relación o vínculo con el Instituto y tengan acceso a sus sistemas de información, recursos tecnológicos o activos digitales del Invima aplican las siguientes acciones:

- Cumplir con lo definido en las políticas y directrices de protección de la información institucionales.
- Informar al grupo Talento Humano sobre terminación o cambios de responsabilidades de los funcionarios.
- Identificar clasificar y valorar los activos de información siguiendo los procedimientos definidos en el sistema de gestión institucional y el Plan Institucional de archivo, así como la inclusión de un nuevo activo de información asociado a sus responsabilidades.
- Controlar el acceso a la información, apoyándose con los controles definidos por el subsistema de gestión de seguridad y las recomendaciones de los grupos de gestión, administrativa, talento humano y contractual.
- Proteger los activos de información contra la pérdida de datos, mediante el apoyo en la definición de respaldos de la información recomendados por la Oficina de tecnologías de información

- Reportar oportunamente y sin demora injustificada los eventos o incidentes de seguridad de la información que evidencies fallas, accesos no autorizados o pérdida de información.
- Identificar, proteger y asegurar el acceso solo a los debidamente autorizados a la información que contiene datos personales según lo establecido en la ley 1581 de 2012.

Oficial de seguridad de la información – Proceso de Gestión de Seguridad de la Información / Representante de la Dirección para el SGSI

Como responsable principal de la implementación del subsistema de gestión de seguridad de la información, el Rol de responsable de la seguridad de la información en el Instituto debe:

- Apoyar al INVIMA en la planificación, diseño, implementación, operación, revisión y mejora continua de los planes de tratamiento de riesgos de seguridad de la información.
- Apoyar al INVIMA en la identificación, selección e implementación de los mecanismos, controles y herramientas tecnológicas necesarias para realizar el tratamiento de riesgos de seguridad de la información.
- Apoyar al INVIMA en el diseño, revisión y actualización de políticas y lineamiento en materia de seguridad de la información.
- Apoyar al INVIMA en las actividades de divulgación y promoción de la importancia del SGSI, los beneficios de la seguridad de la información para la Entidad y las implicaciones de la no conformidad con los requisitos del SGSI.
- Participar en la implementación de los controles de seguridad de la información requeridos por la Entidad para el cumplimiento de sus objetivos.
- Realizar las mediciones de la efectividad de los controles de seguridad de la información implementados.
- Elaborar propuestas de programas de toma de conciencia y formación en seguridad de la información.
- Verificar el cumplimiento de las normas y políticas de seguridad informática de la Entidad, mediante revisiones periódicas del estado de la seguridad de los diferentes servicios, sistemas de información y componentes de tecnología que permiten el tratamiento de la información de la Entidad.
- Verificar el cumplimiento de la seguridad a nivel de operación, desarrollo e implementación de los sistemas de información y las bases de datos.
- Verificar el cumplimiento de la seguridad a nivel de operación de los sistemas de comunicaciones (Red LAN – WAN).
- Coordinar las acciones necesarias para identificar, controlar, reducir y evaluar incidentes de seguridad de la información.
- Participar activamente en la evaluación de los cambios a nivel de infraestructura de tecnología de información y comunicaciones para determinar los riesgos de seguridad, las medidas de mitigación y las acciones correctivas en caso de incidentes de seguridad de la información.
- Participar activamente en la construcción, actualización, mantenimiento y difusión de la documentación que soporta el sistema de gestión de seguridad de la información (SGSI) del INVIMA.
- Realizar valoraciones de riesgos a intervalos periódicos para determinar la efectividad de los controles implementados, las oportunidades de mejora y las acciones correctivas necesarias.
- Apoyar a las diferentes áreas de INVIMA en la identificación y tratamiento de los riesgos de seguridad de la información.

- Atender los eventos e incidentes de seguridad de la información que sean identificados y coordinar a los recursos dispuestos por la Entidad para la identificación, control y recuperación de la Infraestructura de Tecnología de Información y Comunicaciones de la Entidad.
- Investigar, evaluar y recomendar el uso de herramientas de última tecnología que permitan proteger la infraestructura informática de la entidad.
- Apoyar la elaboración y ejecución de los planes operativos anuales y de mejoramiento relacionados con la seguridad informática, de acuerdo con la metodología diseñada por la Entidad.
- Apoyar al INVIMA en las actividades de implementación del Modelo de Privacidad y Seguridad de la información de la estrategia de Gobierno digital.
- Apoyar al INVIMA en las actividades de implementación de la estrategia de ciberdefensa definida por el Ministerio de Defensa Nacional.
- Apoyar los procesos de revisión periódica del panorama de riesgos de seguridad de la información, apoyando la definición de criterios de valoración y aceptación de riesgos de seguridad de la información.
- Elaborar informes del estado de la seguridad de la información, la efectividad de los controles de la seguridad y proponer medidas correctivas y oportunidades de mejora sobre la gestión de la seguridad de la información.
- Preparar la información necesaria para realizar la revisión periódica del estado de la seguridad de la información y acompañar a la Entidad en la revisión de esta para asegurarse de que el sistema de gestión de seguridad de la información permanece conforme a las necesidades de la Entidad y se identifican mejoras al mismo.
- Recolectar, organizar y presentar a la dirección ejecutiva la información sobre el desempeño del SGSI para la preparación de las auditorías internas y la revisión por parte de la Alta Dirección del estado del Subsistema de Gestión de Seguridad de la Información (SGSI).
- Proponer, diseñar y fomentar la implementación de mejoras a los controles y herramientas tecnológicas necesarias para el fortalecimiento de la seguridad de la información en la Entidad.
- Coordinar la realización de acciones correctivas y preventivas para responder a incidentes de seguridad de la información detectados.
- Divulgar las mejoras, acciones correctivas y preventivas a los interesados y partes pertinentes.
- Realizar seguimiento a las mejoras realizadas al sistema de gestión de seguridad de la información y medir su efectividad.
- Apoyar en el levantamiento, actualización y mantenimiento de los activos de información y asociados.
- Apoyar en la identificación, análisis y evaluación de riesgos de seguridad de la información con base en lo establecido en el Sistema de Gestión Integrado.
- Definición, monitoreo y seguimiento del plan de tratamiento de los riesgos de seguridad de la información.
- Definición, monitoreo y seguimiento del plan del Sistema de Gestión y Seguridad de la información.
- Definición, actualización y difusión de las políticas, procesos, procedimientos y formatos del SGSI.
- Definición, monitoreo y seguimiento de los indicadores de seguridad de la información.

- Definición de los planes de entrenamiento y sensibilización para los funcionarios del INVIMA en lo referente a seguridad de la información.
- Apoyar en la evaluación y ajustes de la documentación e información a ser publicada
- Apoyar en la identificación y requerimientos de protección de datos personales

Oficina de tecnologías de la información

- Configurar los límites de acceso a la información con base en los requisitos del INVIMA y de Seguridad de la Información, apoyados por los responsables o coordinadores de cada área, contractual y talento humano.
- Definir ambientes separados de desarrollo, pruebas y operación con el fin de reducir los riesgos de acceso o cambios no autorizados en la operación de los sistemas de información.
- Realizar seguimiento al uso de los recursos, ajustar y proyectar los requisitos de capacidad futura, con el fin de asegurar el desempeño requerido del o los sistemas.
- Prevenir el aprovechamiento de cualquier vulnerabilidad técnica que se pueda presentar, mediante la gestión de la vulnerabilidad técnica.
- Planificar y acordar cuidadosamente auditorías que involucren la verificación de los sistemas operativos.
- Asegurar que la Seguridad de la Información se integre durante todo el ciclo de vida en el proceso de desarrollo y soporte de sistemas de información incluyendo los sistemas de información que prestan servicios sobre redes públicas

Grupo de soporte tecnológico

De conformidad con lo establecido en la resolución número 00500 de marzo 10 de 2021, *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".* El Grupo de soporte tecnológico de INVIMA apoya la implementación del Subsistema de gestión de Seguridad de información a través de las siguientes acciones:

- Propender por realizar las configuraciones seguras que permitan prevenir los riesgos que se puedan presentar por el uso de dispositivos móviles.
- Implementar medidas de aseguramiento a la información que se acceda a través del teletrabajo.
- Definir procedimientos para la gestión de medios removibles cuando se reutilicen, se den de baja y proteger la información que contienen.
- Configurar y limitar el acceso a la información y a las instalaciones de procesamiento de la información con base en los requisitos de INVIMA y de Seguridad de la Información, apoyados por los responsables o coordinadores de cada área, contractual y talento humano.
- Asegurar el uso apropiado y eficaz para proteger la confidencialidad, autenticidad y la integridad de la información mediante el cifrado de la información, apoyados por los responsables o coordinadores de cada área.
- Prevenir la pérdida o acceso no autorizado de información ocasionada por pérdida, daño o robo de equipos o dispositivos móviles que puedan comprometer la información o la operación del INVIMA.
- Realizar seguimiento al uso de los recursos, ajustar y proyectar los requisitos de capacidad futura, con el fin de asegurar el desempeño requerido del o los sistemas.
- Asegurar que la información y las instalaciones de procesamiento de información, se encuentren protegidas contra código malicioso.

- Proteger contra la pérdida de datos, mediante respaldos de la información, software e imágenes de los sistemas, y ponerlas a pruebas regularmente, apoyados por los responsables o coordinadores de cada área.
- Registrar, conservar y revisar los registros acerca de actividades del usuario para generar evidencias de excepciones, fallas y eventos de seguridad de la información.
- Implementar procedimientos para controlar la instalación Software Operacional en los sistemas operativos.
- Prevenir el aprovechamiento de cualquier vulnerabilidad técnica que se pueda presentar mediante la gestión de la vulnerabilidad técnica.
- Planificar y acordar cuidadosamente auditorías que involucren la verificación de los sistemas operativos.
- Asegurar la protección de la información en las redes, sus instalaciones de proceso, protegiéndola al ser transferida mediante cualquier medio.

Gestión de talento humano

De conformidad con los establecido en la Ley 1221 DE 2008 (Julio 16) *"Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones."* El proceso de gestión de Talento humano contribuye a la debida gestión de la seguridad de la información mediante las siguientes acciones:

- Implementar políticas de aseguramiento a la información que se acceda a través del teletrabajo.
- Asegurar que los empleados comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, tomando conciencia de sus responsabilidades en la protección de la información y las cumplan.

Grupo gestión contractual

Para contribuir de manera efectiva a la implementación de un ambiente digital seguro, el grupo de gestión contractual aplica las siguientes acciones:

- Asegurar que los contratistas y proveedores comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, tomando conciencia de sus responsabilidades en la protección de la información.
- Definir y documentar junto con los responsables de la información, acuerdos sobre transferencia segura de información.
- Identificar, revisar regularmente y documentar junto con los responsables de la información, los requisitos para los acuerdos de confidencialidad o no divulgación teniendo en cuenta las necesidades del INVIMA.
- Identificar y definir documentar junto con los responsables de la información, los mecanismos para asegurar la protección de la información que sea accesible a los proveedores.

Oficina asesora de planeación

Para contribuir de manera efectiva a que la gestión de la seguridad de la información sea parte del Sistema Integrado de gestión, la Oficina asesora de planeación aplica las siguientes acciones:

- Definir y asignar de las responsabilidades para la seguridad de la información a todos los procesos institucionales con el apoyo del .
- Orientar la aplicación del procedimiento de gestión de riesgos institucional para que se incorporen las acciones de identificación y

tratamiento de riesgos de seguridad de la información en todos los procesos institucionales.
- Apoyar la identificación de los activos de información de INVIMA y la definición de las responsabilidades de protección apropiadas.
- Definir un control de cambios en el INVIMA aplicados a los procesos de negocio, las instalaciones y en los sistemas de información que afectan la seguridad de la información.
- Impulsar la implementación de controles que aseguren la privacidad y protección de los datos personales como se exige en la ley 1581 de 2012 con el apoyo de las diferentes áreas de la entidad.

Grupo de gestión administrativa

Para contribuir de manera efectiva a que la gestión de la seguridad de la información sea parte del Sistema Integrado de gestión, la Oficina de gestión administrativa aplica las siguientes acciones:

- Verificar la entrega por parte de los servidores públicos y contratistas de todos los activos asociados con la información e instalaciones de procesamiento.
- Implementar acciones de control para prevenir el acceso físico no autorizado a las áreas identificadas como críticas por la información que contienen, administran o generan.
- Identificar, definir y documentar junto con los responsables de la información, los mecanismos para asegurar la protección de la información que sea accesible a los proveedores.

Grupo de gestión documental y correspondencia

El grupo de gestión documental y correspondencia apoya la gestión de la seguridad de la información con acciones orientadas a:

- Apoyar la identificación de los activos de información de INVIMA y la definición de las responsabilidades de protección apropiadas.
- Implementar y documentar un procedimiento para el etiquetado de la información, de acuerdo con el esquema de clasificación de la información adoptado por INVIMA.
- Proteger contra el acceso no autorizado, uso indebido o corrupción durante el transporte, los medios que contienen información.

Oficina asesora jurídica

La oficina asesora jurídica, apoya la gestión de la seguridad de la información con acciones orientadas a:

- Definir y documentar junto con los responsables de la información, acuerdos sobre transferencia segura de información.
- Identificar, revisar regularmente y documentar junto con los responsables de la información, los requisitos para los acuerdos de confidencialidad o no divulgación, teniendo en cuenta las necesidades de INVIMA.
- Asesorar con el fin de evitar el incumpliendo en las obligaciones legales o contractuales relacionadas con la seguridad de la información.

Oficina de control interno

La Oficina de Control Interno, en el marco de sus funciones establecidas en la normatividad vigente, tendrá las siguientes responsabilidades frente a la Seguridad de la Información:

1. Evaluación independiente

- Evaluar de manera objetiva e independiente la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la

Información (SGSI).
- Verificar la adecuada gestión de los riesgos de seguridad de la información por parte de la entidad.

2. Seguimiento y control

- Realizar seguimiento periódico al cumplimiento de la Política de Seguridad de la Información y sus lineamientos asociados.
- Verificar la implementación de controles de seguridad definidos para mitigar riesgos.

3. Auditoría interna

- Incluir dentro del Plan Anual de Auditoría evaluaciones relacionadas con la seguridad de la información.
- Auditar el cumplimiento de:
  - Políticas y procedimientos de seguridad
  - Normativa aplicable (Ley 1581 de 2012, Ley 1712 de 2014, lineamientos MinTIC, entre otros)
  - Controles establecidos en el SGSI

4. Verificación del cumplimiento normativo

- Validar que la entidad cumpla con las disposiciones legales y regulatorias en materia de:
  - Protección de datos personales
  - Transparencia y acceso a la información pública
  - Gobierno Digital
  - Seguridad digital

5. Emisión de recomendaciones

- Formular recomendaciones orientadas al fortalecimiento del control interno en materia de seguridad de la información.
- Promover la mejora continua del SGSI sin asumir funciones de administración o implementación.

6. Reporte a la alta dirección

- Informar a la Alta Dirección sobre:
  - Resultados de auditorías
  - Hallazgos y brechas de seguridad
  - Nivel de madurez del control interno en seguridad digital

7. Fomento de la cultura de control

- Contribuir al fortalecimiento de la cultura de control y autocontrol en la entidad, incluyendo aspectos relacionados con la seguridad de la información.

Grupo de control disciplinario interno	• El grupo de control disciplinario interno facilitara la aplicación de las obligaciones en materia de seguridad de la información aplicando el código general disciplinario cuando se identifiquen acciones que puedan constituir violaciones a los deberes de los servidores públicos en materia de seguridad de la información.
Misionales y Oficina de Laboratorios y control de Calidad	Para contribuir de manera efectiva a que la gestión de la seguridad de la información sea parte del Sistema Integrado de gestión, los procesos y áreas misionales, la oficina de laboratorios y de control de calidad, aplican las siguientes acciones: • Velar por la protección de la información bajo su custodia, asegurando su confidencialidad, integridad y disponibilidad, así como la gestión de riesgos y el cumplimiento de la normatividad vigente en materia de seguridad de la información asociado a sus responsabilidades • Asegurar la protección de los datos personales y la transparencia, en particular en la Oficina de Laboratorios de Calidad, la cual deberá garantizar la trazabilidad, confiabilidad e integridad de los resultados analíticos y de la información científica generada, mediante la implementación de controles técnicos y administrativos que aseguren la validez de los resultados, el control y respaldo de los datos y registros, y la trazabilidad metrológica, de acuerdo con los requisitos de la norma ISO/IEC 17025 vigente, preservando la seguridad, confidencialidad y disponibilidad de la información durante todo su ciclo de vida. • Reportar oportunamente y sin demora injustificada los eventos o incidentes de seguridad de la información que evidencien fallas, accesos no autorizados, modificaciones o pérdida de información.

7. PRINCIPIOS

La actuación del Instituto y de todos sus colaboradores se rige por los siguientes principios de transparencia, seguridad y privacidad de la información:

- **Disponibilidad:** Garantía de que la información y los recursos asociados sean accesibles y utilizables de manera oportuna por las entidades, usuarios o procesos debidamente autorizados, cuando así se requiera.
- **Confidencialidad:** Propiedad que asegura que la información no sea divulgada ni puesta a disposición de personas, entidades o procesos no autorizados, protegiendo su acceso de manera adecuada.
- **Integridad:** Propiedad que salvaguarda la exactitud, consistencia y completitud de la información y sus métodos de procesamiento, evitando modificaciones no autorizadas.
- **Autenticidad:** Propiedad que garantiza que la identidad de un sujeto, sistema, recurso o información es válida y corresponde a la declarada, asegurando la confiabilidad en las interacciones y transacciones.
- **Legalidad**: Propiedad que trata la información, en especial de los datos personales, en estricto cumplimiento de la normatividad vigente aplicable, incluyendo las disposiciones constitucionales, legales y regulatorias en materia de protección de datos y acceso a la información pública.
- **Transparencia**: Propiedad que garantiza que los titulares de la información puedan conocer, actualizar y solicitar información sobre el tratamiento de sus datos personales en cualquier momento, en concordancia con los principios de acceso a la información pública y rendición de cuentas.

8. MECANISMOS DE COMUNICACIÓN DE LA PRESENTE POLÍTICA

La presente política será socializada a los servidores públicos, contratistas y demás colaboradores del Instituto a través de los canales de comunicación disponibles en la Entidad y estará disponible para consulta a través del portal web y de la plataforma integra.

9. DEFINICIONES EN EL MARCO DE LA SEGURIDAD DE LA INFORMACION

- **Activo de 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, etc.) que tenga valor para la organización.
- **Amenaza**: Posible causa de un incidente no deseado, que puede producir daño a un sistema u organización.
- **Análisis de riesgos**: Proceso de comprender la naturaleza, el nivel del riesgo y establecer las bases para su tratamiento.
- **Brecha de Seguridad**: Evento en el cual la información es accedida, divulgada o alterada sin autorización.
- **Confidencialidad**: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Control (es):** Medida que modifica el riesgo. Sinónimo salvaguarda.
- **Control de Acceso:** Mecanismo que limita el acceso a las instalaciones físicas, sistemas e información según permisos establecidos.
- **Copia de Seguridad (Backup):** Copia de la información realizada para garantizar su recuperación en caso de pérdida o incidente.
- **Gestión de riesgos**: Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone del proceso de identificación, análisis, evaluación y tratamiento de riesgos relacionados con la seguridad de la información.
- **Información**: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen Ley 1712/2014
- **Disponibilidad**: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Integridad**: Propiedad de la información que busca preservar su exactitud y completitud.
- **Parte interesada (Stakeholder)**: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).
- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información**: Es el conjunto de políticas, manuales, procedimientos, procesos, recursos, técnicas y controles orientados a gestionar de manera sistemática los riesgos asociados a la seguridad de la información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información.
- **Tercero**: hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una amenaza.

10. DOCUMENTO ASOCIADOS

- GSSI-PRO4-PROCEDIMIENTO GESTIÓN DE INCIDENTES (GSSI-PRO4)
- GSSI-PRO1-PROCEDIMIENTO INVENTARIO DE ACTIVOS DE INFORMACIÓN (GSSI-PRO1)
- GSSI-INS1-INSTRUCTIVO DE RELACIÓN CON AUTORIDADES Y GRUPOS DE INTERÉS (GSSI-INS1)
- GSSI-FOR1-MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN (GSSI-FOR1)

CONTROL DE CAMBIOS

Versión	Fecha	Usuario	Comentario
2	03/08/2026	Adriana Ruth Gaitán Urquijo	inicia ruta documental para actualizaciones aprobadas en cuanto a ajuste del nombre y la información contemplada en la de acuerdo a la nueva estructura de políticas institucionales

ELABORÓ	REVISÓ	APROBÓ
Nidia Nayibe Gonzalez Pinzon **Coordinador Grupo Soporte Tecnológico** Felix Alberto Rozo Lara **Contratista** **Fecha de elaboración:** 03/08/2026	Maria Del Pilar Nieto Cespedes **Profesional Universitario Oficina de Laboratorios y Control de Calidad** Adriana Ruth Gaitán Urquijo **Profesional Universitario Grupo de Gestión y Mejoramiento Organizacional** Laura Carolina Castellanos Portillo **Planta** **Fecha de revisión:** 03/08/2026	Francisco Augusto Giuseppe Rossi Buenaventura **Director General** **Fecha de aprobación:** 03/08/2026