1. INTRODUCCIÓN

La política de seguridad de la información muestra la postura del Instituto Nacional de Vigilancia de Medicamentos y Alimentos - INVIMA en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad del organismo en cuanto a la seguridad de la información. Esta política debe garantizar la calidad de la información y la prestación continua de los servicios, supervisando la actividad diaria y reaccionando con certeza ante cualquier incidente; esto con la finalidad de identificar, evaluar y controlar los riegos que pudiesen afectar la confidencialidad, integridad y disponibilidad de la información dentro de la entidad.

2. OBJETIVO

Establecer los lineamientos definidos por la Dirección del INVIMA para la seguridad de la información y la protección de los datos personales, teniendo en cuenta las condiciones de uso confiable de la información y el dato, su entorno digital y físico; realizando una adecuada gestión de los riesgos, preservando la confidencialidad, integridad y disponibilidad de la información y dato tratado, y de los servicios que se prestan al ciudadano, todo lo anterior teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información -MSPI, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

3. DEFINICIONES

Activo: 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 del riesgo y determinar su nivel de riesgo.
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.
Gestión de riesgos: Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
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 manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
Tercero: hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA reconoce la seguridad de la información y la protección de los datos personales requeridos en los procesos de vigilancia y control sanitario debe ser preservada en su confidencialidad, integridad y disponibilidad, por lo que el INVIMA se compromete a proteger la información procurando mantener un nivel del riesgo que permita responder por la integridad, confidencialidad, autenticidad y disponibilidad de la información, implementando los controles necesarios que permitan mitigarlos.
El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA se compromete con la sensibilización, educando y comprometiendo a su recurso humano en el manejo seguro de la información, cumpliendo con los requisitos legales y demás aplicables a todo el sistema integrado de gestión, implementando los controles efectivos que faciliten el cumplimiento de la misión institucional y el mejoramiento continuo.

4.OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

Garantizar la gestión adecuada de la seguridad de la información tratada en el fortalecimiento de la inspección vigilancia y control sanitario, contribuyendo a una Colombia legal y transparente mediante la implementación de acciones que mitiguen los efectos de la ilegalidad y la corrupción, con enfoque de riesgo garantizando la protección de la salud de los colombianos y el Reconocimiento nacional e internacional.
Establecer los lineamientos de seguridad de la información necesarios que apoyen la gestión efectiva y transparente que ayuden a incrementar la importancia, credibilidad y confianza en el INVIMA.
Proteger la información, promoviendo siempre la aplicación de las mejores prácticas de seguridad de la información de manera responsable, teniendo en cuenta el valor implícito que tienen los recursos financieros, humanos, físicos y ambientales utilizados en el INVIMA.
Establecer una cultura entre los funcionarios, terceros, aprendices, practicantes y grupos de interés del INVIMA del tratamiento seguro de la información.
Identificar y procurar los mecanismos técnicos, tecnológicos y de personal para atender y minimizar los riesgos de seguridad de la información de todos los procesos del Invima.
Mejorar continuamente el sistema de gestión de seguridad de la información a través de las lecciones aprendidas y los sucesos, eventos o novedades que se presenten en materia de protección y amenazas que afecten la disponibilidad, integridad y confidencialidad de la información.
Diseñar y/o Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.

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. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información conforme a los requisitos normativos comprende a todos los procesos de la entidad.

7. APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, servidores públicos, contratistas y terceros del INVIMA.
El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa del Instituto.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

El Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.…): ROL / INSTANCIA / DEPENDENCIA RESPONSABILIDADES (los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)

Macroproceso / Proceso / Rol	Responsabilidades
Dirección general	• La dirección debe mostrar liderazgo y compromiso frente al SGSI, asegurando que se establezca la política del Sistema de Gestión de Seguridad de la Información y los objetivos de este, siendo estos definidos de acuerdo con la misión y visión

Macroproceso / Proceso / Rol	Responsabilidades
	de la entidad. • Apoyar la integración del SGSI con los procesos de la entidad, garantizando recursos económicos y de personal, así como impulsar y asegurar que todos los servidores públicos y contratista conozcan y apliquen las políticas y procedimientos establecidos en temas de seguridad de la información • Asegurarse de hacer seguimiento a la implementación del sistema de gestión de seguridad de la información y que este logre los resultados previstos con eficacia. • Apoyar y velar por la formación de Auditores Internos en NTC ISO 27001:2013. • Asegurar, que las responsabilidades para los roles de la Seguridad de la información se asignen y comuniquen.
Comité institucional de desarrollo y desempeño	• Este comité debe estar integrado por los miembros del comité institucional de desarrollo, y sus obligaciones son las siguientes: • 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 los planes de tratamiento de riesgos de seguridad de la información. • Aprobar los programas de pruebas y análisis de vulnerabilidades de la infraestructura tecnológica. • Verificar el cumplimiento de las políticas de seguridad y emitir recomendaciones sobre la materia. • Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. • Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes. • Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
Oficial de seguridad de la información – Proceso de Gestión de Seguridad de la Información / Representante de la Dirección para el SGSI	• 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 a 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 a INVIMA en las actividades de implementación del Modelo de Privacidad y Seguridad de la información de la estrategia de Gobierno digital. • Apoyar a 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.

Macroproceso / Proceso / Rol	Responsabilidades
	• Realizar seguimiento a las mejoras realizadas al sistema de gestión de seguridad de la información y medir su efectividad. • Apoyo en el levantamiento, actualización y mantenimiento de los activos de información y asociados. • Apoyo 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. • Apoyo en la evaluación y ajustes de la documentación e información a ser publicada • Apoyo 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	• Garantizar 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/o 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 de 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	• 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	• 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 de 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	• Definir y asignar las responsabilidades para la seguridad de la información. • Integrar los métodos de gestión de proyectos de la organización, con el fin de asegurar que los riesgos de seguridad de la información sean identificados y tratados como parte de cualquier proyecto, independientemente de su naturaleza. • 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 INVIMA aplicados a los procesos de negocio, las instalaciones y en los sistemas de información que afectan la seguridad de la información. • Incluir la continuidad de la seguridad de la información aún en la ejecución de contingencia, definida en el sistema de gestión de continuidad de negocio.

Macroproceso / Proceso / Rol	Responsabilidades
	• Asegurar la privacidad y protección de los datos personales como se exige en la ley 1581 con el apoyo de las diferentes áreas de la entidad.
Grupo de gestión administrativa	• Garantizar la verificación de entrega por parte de los servidores públicos y contratistas de todos los activos asociados con la información e instalaciones de procesamiento. • 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	• 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	• 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	• Apoyar en la revisión Independiente de la seguridad de la Información (Contratar un externo para auditorías internas). • Formar Auditores Internos en la norma
Grupo de control disciplinario interno	• Incluir dentro del proceso normal las violaciones a la seguridad de la información.
Procesos y áreas (servidores públicos y contratistas)	• Cumplir con lo definido en las políticas y directrices de protección de la información. • Informar a Talento Humano sobre terminación o cambios de responsabilidades de los funcionarios. • Identificar clasificar y valorar los activos de información. • Controlar el acceso a la información, apoyándose con TI, Administrativa, talento humano y contractual. • Proteger contra la pérdida de datos, mediante el apoyo en la definición de respaldos de la información y sus respectivas pruebas regularmente, junto con TI. • Reportar eventos o incidentes de seguridad de la información que evidencies fallas, accesos no autorizados o pérdida de información. • Identificar la información que contiene datos personales, teniendo en cuenta la ley 1581.

â€‹â€‹â€‹â€‹â€‹â€‹â€‹9. **MANEJO DE DESVIACIONES Y EXCEPCIONES**
Las desviaciones presentadas por el Subsistema de Gestión de Seguridad de la Información serán manejadas de acuerdo con la Política y el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

Las excepciones a las políticas, procedimientos y controles del Subsistema de Gestión de Seguridad de la información deben ser evaluadas por el Oficial de Seguridad de la Información, teniendo en cuenta:

- El evento que genera la excepción.
- Los posibles riesgos que puedan presentarse con la excepción.
- El posible impacto que pueda generar a excepción.
- Las acciones para el manejo de la excepción.

Las excepciones según su nivel deben tener el visto bueno del líder de proceso y la evaluación y autorización del Oficial de Seguridad de la Información y/o el comité institucional de Gestión y Desempeño.

10. **FECHA DE ENTRADA EN VIGENCIA DE LA POLITICA**
La presente política es adoptada por medio de acta de Comité Institucional de Gestión y Desempeño número 008 del 23 de septiembre de 2024.

CONTROL DE CAMBIOS

Versión	Fecha	Usuario	Comentario
2	17/12/2024	Mary Jazmin Luengas Moreno	Se solicita nueva versión para garantizar la eficacia y adaptabilidad frente a los cambios internos y externos, como también el de salvaguardar los activos de información de la entidad con las ultimas actualizaciones indicadas por el Ministerio de las Tecnologías de la Información Â- MIN TIC.

ELABORÓ	REVISÓ	APROBÓ

GDI-DIE-PL24-POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código	GDI-DIE-PL24
Versión	2
Tipo	Política
Implementación	23/09/2024
Alcance	Invima
Nivel de confidencialidad	Público

Ferney Alejandro Ramirez Mora **Contratista de Grupo de Gestión y Mejoramiento Organizacional** **Fecha de elaboración:** 23/09/2024	Maria del Pilar Hidalgo Alferez **Coordinador Grupo de Gestión y Mejoramiento Organizacional** Jina Marcela Lozano Bedoya **Jefe Oficina Asesora de Planeación** Nidia Nayibe Gonzalez Pinzon **Contratista** **Fecha de revisión:** 23/09/2024	Francisco Augusto Giuseppe Rossi Buenaventura **Director General** **Fecha de aprobación:** 23/09/2024