POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL INVIMA

1. INTRODUCCIÓN

La Política General de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del INVIMA con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la entidad y apoyan la implementación del Subsistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.
El Subsistema de Gestión de Seguridad de la Información (SGSI) hace parte del Sistema Integrado de Gestión del INVIMA. Este subsistema contiene las políticas técnicas, procedimientos, directrices, metodologías y controles necesarios para la efectiva gestión de la seguridad de la información, alineados con lo estipulado por la política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión, el Modelo de Seguridad y Privacidad de la Información y la norma ISO 27001 como referencia.

2. OBJETIVO

Establecer las condiciones de uso confiable de la información el entorno digital y físico, realizando una adecuada gestión de los riesgos, preservando la confidencialidad, integridad y disponibilidad de la información tratada, y de los servicios que se prestan al ciudadano.

3. OBJETIVOS ESPECÍFICOS

- 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.
- Gestionar oportuna y adecuadamente los riesgos de seguridad de la información INVIMA.

4. ALCANCE

La Política General de Seguridad y Privacidad de la Información es adoptada por todos los procesos, procedimientos, y tratamientos de información que realice el INVIMA, a terceros que traten información en nombre de la entidad, a quienes se transfiera o trasmita información cuyo responsable sea el instituto.

5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El INVIMA reconoce la seguridad de la información requerida en los procesos de vigilancia y control sanitario preservando la confidencialidad, integridad y disponibilidad de la información, realizando una adecuada gestión de los riesgos que afectan la información, implementando los controles necesarios que permitan mitigarlos, sensibilizando, educando y comprometiendo a su recurso humano en el manejo seguro de la información, con la apropiación de los requisitos legales, las necesidades del instituto y de las partes interesadas en seguridad de la información.

6. TÉRMINOS Y DEFINICIONES

Las definiciones de la Política General de Seguridad y Privacidad de la Información del INVIMA, tiene fundamento en el estándar internacional ISO 27000.
A continuación, se listan algunas de las más importantes, relacionadas con la gestión de los documentos:

- **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 de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Medida que modifica el riesgo. Sinónimo salvaguarda.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **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
- **Integridad:** La propiedad de salvaguardar la exactitud y complejidad de la información.
- **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 (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o 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.

7. MARCO NORMATIVO

- **Ley 527 de 1999 Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos:** El mensaje de datos es “La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax”.
- **Ley 594 de 2000 Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones:** Responsabilidad “Los servidores públicos son responsables de la organización, conservación, uso y manejo de los documentos”.
- Administración y acceso. “Es una obligación del Estado la administración de los archivos públicos y un derecho de los ciudadanos el acceso a los mismos, salvo las excepciones que establezca la ley;”

- **Ley 599 DE 2000 Por la cual se expide el Código Penal:** En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."
- **Ley 734 de 2002 Por la cual se expide el Código Disciplinario Único:** Art 34. Deberes. Son deberes de todo servidor público "4. 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. 5. 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. "
- **La Ley 850 de 2003 Por medio de la cual se reglamentan las veedurías ciudadanas:** Principio de Transparencia "A fin de garantizar el ejercicio de los derechos, deberes, instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia".
- **Ley 962 de 2005 Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos:** Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
- **Ley 1150 de 2007 Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos:** Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Secop.
- **Ley 1266 de 2008 Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países:** Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;
- **Ley 1221 de 2008 Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones**: Teletrabajo. Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.
- **Ley 1273 de 2009 Por medio de la cual 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:** "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"
- **Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009 Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones:** Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.
- **Ley 1581 de 2012 Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales**: Se hace referencia, principalmente, al artículo 15 de la Constitución Nacional en el cual se establece que "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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución…".
- **Decreto 884 de 2012 Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones:** El empleador debe informar al tele trabajador sobre las restricciones de uso de equipos y programas informáticos, la legislación vigente en materia de protección de datos personales, propiedad intelectual, seguridad de la información y en general las sanciones que puede acarrear por su incumplimiento.
- **Decreto 886 de 2014 Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos:** Serán objeto de inscripción en el Registro Nacional de Bases de Datos, "las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2° de la Ley 1581 de 2012".
- **Decreto Nacional 2573 de 2014 Estrategia de Gobierno en Línea de la República de Colombia:** E, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad
- **Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública:** Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley".
- **Decreto 103 de 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones:** "La información pública que contiene datos semiprivados o privados, definidos en los literales g) y h) del artículo 3° de la Ley 1266 de 2008, o datos personales o sensibles, según lo previsto en los artículos 3° y 5° de la Ley 1581 de 2012 y en el numeral 3° del artículo 3° del Decreto 1377 de 2013, solo podrá divulgarse según las reglas establecidas en dichas normas."
- **Ley 1952 del 2019 por la cual se expide el código general disciplinario** que deroga la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario. Artículo 38 deberes. son deberes de todo servidor público: "5. utilizar los bienes y recursos asignados para el desempeño de su empleo cargo función, las facultades que les sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines que están afectos. 6. custodiar y cuidar la documentación e información que, por razón de su empleo, cargo función conserve bajo su cuidado OA la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos, dentro del Marco Normativo de la Política General de Seguridad y Privacidad de la Información.
- **CONPES 3701 Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país:** Este documento define un plan de acción para la ejecución de la política en ciberseguridad y ciberdefensa, el cual estará a cargo de las entidades involucradas, fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa), creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se formularon tres objetivos específicos: (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional; (ii) brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad; y (iii) fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.
- **CONPES 3854 por el cual se crea y justifica la Política Nacional de Seguridad Digital:** El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países.
- **Decreto 1499 del 11 de septiembre de 2017 Integración del Sistema de Gestión de Calidad y lo Sistemas de desarrollo administrativo:** 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.
- **Decreto 25 de agosto de 2017 Los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administración pública a través de medios electrónicos**: Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones.

8. **RESPONSABILIDADES**

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 de la entidad.

Macroproceso / Proceso / Rol	Responsabilidades
	• 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.

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 006 del 01 de noviembre de 2022 y rige a partir de esta fecha.

ELABORÓ	REVISÓ	APROBÓ
Nidia Nayibe Gonzalez Pinzon **Contratista** **Fecha de elaboración:** 01/11/2022	Daladier Medina Niño **Jefe Oficina Asesora de Planeación** **Fecha de revisión:** 01/11/2022	Francisco Augusto Giuseppe Rossi Buenaventura **Director General** **Fecha de aprobación:** 01/11/2022