PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., enero de 2021

Instituto Nacional de Vigilancia de Medicamentos y Alimentos - Invima
Oficina Principal: Cra 10 N° 64 - 28 - Bogotá
Administrativo: Cra 10 N° 64 - 60
(1) 2948700
www.invima.gov.co

Contenido

1 ALCANCE DEL PLAN

La implementación, gestión y operación del Sistema de Gestión de Seguridad de la Información - SGSI, se realiza en todos los procesos del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, de acuerdo con el ciclo de mejora continua PHVA; esto incluye, las actividades de formalización de los procesos, procedimientos y documentación correspondiente al SGSI a través de su integración con el Sistema de Gestión Integrado – SGI donde se manifiesta lo siguiente:

"El Invima diseña, promueve y adoptas las medidas necesarias que permitan disponer, gestionar y proteger la información suministrada a la entidad y generada por la misma de las diferentes amenazas que pueden afectar la integridad, disponibilidad y confidencialidad de la información. Identificando y gestionando los riesgos de forma eficiente y efectiva en todos los procesos, incorporando como resultado de esta gestión la mejora continua en materia de seguridad de la información, entendiendo que esta puede encontrarse en medios electrónicos y físicos."

2 OBJETIVO

Este plan tiene como objetivo determinar las acciones que se realizaran para proteger la información que el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA utiliza para 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.

3 OBJETIVOS ESPECÍFICOS

- Revisar, actualizar las políticas y documentos existentes
- Divulgar e implementar el SGSI
- Hacer seguimiento al cierre de brechas resultado de la auditoría interna
- Definir indicadores
- Evaluar el SGSI
- Certificar el SGSI

4 ESTRATEGIAS

Teniendo en cuenta el objetivo estratégico del instituto de 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. Así como los objetivos estratégicos de la entidad:

- Contribuir a la mejora continua del estatus sanitario del país mediante el fortalecimiento de la inspección, vigilancia y control sanitario con enfoque de riesgo

garantizando la protección de la salud de los colombianos y el reconocimiento nacional e internacional
- Prestar servicios con estándares de calidad para afianzar la confianza de la población
- Fortalecer la gestión del conocimiento, capacidades y competencias de los servidores públicos de la institución
- Contribuir a una Colombia legal y transparente mediante la implementación de acciones que mitiguen los efectos de la ilegalidad y la corrupción

Se plantean las siguientes estrategias en la implementación del Sistema de Gestión de Seguridad de la Información:

1- Sensibilizar a las diferentes áreas y procesos de la entidad sobre las responsabilidades que tienen frente a la protección y acceso a la información.
2- Generar alianzas entre procesos de apoyo que administren y gestionen controles de acceso de usuarios de forma física y digital, para garantizar el cumplimiento de las directrices de control de acceso establecidas en el SGSI.
3- Implementar acciones que permitan cerrar las brechas encontradas en la auditoría interna realizada en el 2020.
4- Capacitar a los servidores públicos en la identificación y tratamiento de los riesgos de seguridad de la información y la identificación de los activos de información, así como su valoración.

5 PROYECTOS

Dentro de los proyectos establecidos para seguridad de la información se encuentra la contratación de un ethical hacking y la realización de una auditoría interna, con miras a que la entidad se pueda certificar en la norma ISO 27001:2013; a continuación, se especifican los requerimientos y necesidades de estos dos proyectos:

5.1 CIERRE DE BRECHAS ENCONTRANDAS EN LA REVISIÓN TÉCNICA INDEPENDIENTE DEL 2020

Elaborar junto con el grupo de soporte tecnológico y la oficina de tecnologías de la información un plan de acción para la mitigación de todas las vulnerabilidades encontradas en el ejercicio del hacking ético.

Realizar un retest del hacking ético en búsqueda de vulnerabilidades que nos permita identificar si las brechas de seguridad que afectan la tecnología fueron debidamente tratadas y cerradas, así como identificar si existen nuevas vulnerabilidades que deban ser tratadas.

5.2 CIERRE DE BRECHAS DE AUDITORÍA REALIZADA EN EL 2020

De acuerdo con los resultados de la auditoría interna realizada por la oficina de control interno al sistema de gestión de seguridad de la información es necesario realizar las siguientes acciones:

Elaborar junto con la oficina asesora de planeación, el grupo de soporte tecnológico y la oficina de tecnologías de la información, un plan que permita cerrar las 12 no conformidades encontradas con base a los requisitos de norma ISO 27001:2013, que a su vez dan cumplimiento con lo estipulado en el DAFP, el FURAG y el Modelo de Privacidad y seguridad de la información MPSI.

Elaborar junto con la oficina asesora de planeación, el grupo de soporte tecnológico y la oficina de tecnologías de la información un plan que permita mitigar los riesgos de una no conformidad en cumplimiento de norma, teniendo en cuenta las 2 oportunidades de mejora identificadas en la auditoria interna realizada al sistema de gestión de seguridad de la información.

5.3 REVISIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con el de continuar con el ejercicio ya realizado durante el periodo del 2020, dando cumplimiento a las obligaciones que como entidad del estado se tienen frente al MINTIC, DAFP, las evaluaciones del FURAG, la aplicación de MIPG, así como las obligaciones legales o de reglamentación relacionadas con seguridad de la información, es necesario junto con control interno realizar la segunda auditoría interna al sistema de gestión de seguridad de la información.

Se proyecta que dentro de la formación al grupo de auditores internos se incluya el sistema de gestión de seguridad de la información SGSI y su respectiva auditoría.

Se proyecta que dentro de la formación al personal y en miras de la apropiación por parte del personal en temas de protección de la información, se cuente con una formación en seguridad de la información (Norma ISO 27001:2013 y Sistema de gestión de seguridad de la información), protección de datos personales (ley 1581 de 2012, ley para la protección de los datos personales).

5.4 REVISIÓN POR LA DIRECCIÓN DEL AVANCE DEL PLAN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que una de las no conformidades encontradas en la auditoría se relacionaba con la revisión por la dirección, se plantean 4 revisiones por la dirección en el año 2021, donde se deberá:

1- Socializar el avance de implementación del presente plan.
2- Dar a conocer el seguimiento al plan de tratamiento de riesgos de seguridad de la información.
3- Identificar los requerimientos de apoyo o intervención por parte de la dirección.
4- Seguimiento a indicadores del SGSI.

6 METAS

Dentro de las metas planteadas en la implementación del Sistema de Gestión de Seguridad de la Información y acordes al MSPI se definen las siguientes metas:

- Los Servidores públicos y contratistas, reconocen y son informados sobre sus responsabilidades frente a la protección de la información al realizar trabajo en casa y/o teletrabajo
- Integración entre los procesos de apoyo que administran y gestionan controles de acceso físico y digital, con el fin de garantizar el cumplimiento de las directrices de control de acceso establecidas en el sistema de gestión de seguridad de la información.
- Los servidores públicos y contratistas tienen la capacidad de identificar y documentar los riesgos de seguridad de la información a partir del inventario de activos de información valorado y clasificado.

7 ACCIONES

Las acciones se encuentran especificadas por fases de acuerdo con el avance de la implementación del SGSI y se presentan a continuación:

Nombre Fase 1: Socialización y planificación
Presentación de proyecto a Comité Institucional de Gestión y Desempeño, para aprobación de proyecto de implementación de Sistema de Gestión de Seguridad de la Información -SGSI.
Asumir compromiso por parte del Invima para continuar con la implementación y certificación de SGSI.
Divulgación a nivel institucional del compromiso adquirido de implementación y certificación de SGSI
Generación de ajustes a la documentación al interior de los procesos y planes operativos de la entidad para cumplir con la implementación y certificación de SGSI

Socialización de avances al comité Institucional de Gestión y Desempeño del presente Proyecto y sus Objetivos
Diagnosticar y Analizar de la situación de la entidad frente a Seguridad de la información
Planificación de implementación del SGSI

Nombre Fase 2: Implementación de SGSI
Creación del proceso SGSI
Documentación de Procedimientos e instructivos requeridos para la implementación de SGSI.

Nombre Fase 3: Revisión independiente de la seguridad de la información
Revisión del cumplimiento técnico
Auditoría interna del SGSI
Implementación de Mejoras
Socialización de resultados al comité Institucional de Gestión y Desempeño

Nombre Fase 4:
Solicitud de certificación
Certificación de SGSI implementado

8 PRODUCTOS

El principal producto del presente plan será el Sistema de Gestión de la Seguridad de la Información certificado bajo la norma ISO 27001:2013

A continuación, se presentan los entregables durante el desarrollo del proyecto

Nombre Fase 1: Socialización y planificación	Entregables
Presentación de proyecto a Comité Institucional de Gestión y Desempeño, para aprobación de proyecto de implementación de Sistema de Gestión de Seguridad de la Información -SGSI.	Documentación existente del SGSI, presentación power point y Acta
Asumir compromiso por parte del Invima para continuar con la implementación y certificación de SGSI.	Acta
Divulgación a nivel institucional del compromiso adquirido de implementación y certificación de SGSI	Campaña de comunicaciones
Generación de ajustes a la documentación al interior de los procesos y planes operativos de la entidad para cumplir con la implementación y certificación de SGSI	Documentación revisada y actualizada
Socialización de avances al comité Institucional de Gestión y Desempeño del presente Proyecto y sus Objetivos	Actas
Diagnosticar y Analizar de la situación de la entidad frente a Seguridad de la información	Documentos de autodiagnóstico (FURAG, MSPI, MIPG)
Planificación de implementación del SGSI	Documento Plan del SGSI

Nombre Fase 2: Implementación de SGSI	Entregables
Creación del proceso SGSI	Proceso credo en el mapa de procesos
Documentación de Procedimientos e instructivos requeridos para la implementación de SGSI.	Documentos diseñados para el SGSI

Nombre Fase 3: Revisión independiente de la seguridad de la información	Entregables
Revisión del cumplimiento técnico	Informes de resultados de la revisión técnica
Auditoría interna del SGSI	Informe de Auditoría
Implementación de Mejoras	Acciones de mejora implementadas y documentadas (Presupuesto de soporte tecnológico y tecnologías de la información)
Socialización de resultados a la comité Institucional de Gestión y Desempeño	Acta

Nombre Fase 4 (2022)	Entregables
Solicitud de certficación	Documentación pertinente
Certificación de SGSI implementado	Certificado del ente certificador

9 RESPONSABLES

En la definición de los responsables y responsabilidades se identificaron para el plan las siguientes

Gerente de Programa	Daladier Medina Niño			
Gerente del Proyecto	Nidia Nayibe Gonzalez P			
Líder del Subproyecto	Maria del Pilar Hidalgo			
Dependencias que participan en el desarrollo del proyecto	Dirección General	Oficina de Tecnologías de la Información	Oficina de Atención al Ciudadano	Dirección de Dispositivos Médicos y Otras
	Secretaría General	Oficina de Control Interno	Dirección de Medicamentos y Productos Biológicos	Dirección de Cosméticos, Aseo, Plaguicidas y
	Oficina Asesora de Planeación	Oficina Asesora Jurídica	Dirección de Alimentos y Bebidas	Dirección de Operaciones Sanitarias

Además de las responsabilidades específicas ya definidas de acuerdo con lo estipulado en el anexo de la norma ISO 27001:2013, que a continuación se recuerdan:

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.
- 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.

Oficina De Tecnologías de la Información

- Configurar los límites de acceso a 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 de acuerdo con lo estipulado en el Dominio A.9.
- Definir ambientes separados 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 de acuerdo con lo estipulado en el Anexo A.12.1.4.
- Realizar seguimiento al uso de los recursos, ajustar y proyectar los requisitos de capacidad futra con el fin de asegurar el desempeño requerido del o los sistemas de acuerdo con lo estipulado en el Anexo A.12.1.3.
- Prevenir el aprovechamiento de cualquier vulnerabilidad técnica que se pueda presentar mediante la gestión de la vulnerabilidad técnica de acuerdo con lo estipulado en el Anexo A.12.6.
- Planificar y acordar cuidadosamente auditorías que involucren la verificación de los sistemas operativos de acuerdo con lo estipulado en el Anexo A.12.7.
- 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 de acuerdo con lo estipulado en el dominio A.14.

Grupo de Soporte Tecnológico

- Garantizar las configuraciones seguras que permitan prevenir los riesgos que se puedan presentar por el uso de dispositivos móviles de acuerdo con lo estipulado en el Anexo A.6.2.1.
- Implementar medidas de aseguramiento a la información que se acceda a través del teletrabajo de acuerdo con lo estipulado en el Anexo A.6.2.2.
- Definir procedimientos para la gestión de medios removibles cuando se reutilicen, se den de baja y proteger la información que contienen, acuerdo con lo estipulado en el Anexo A.8.3.1.
- 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 de acuerdo con lo estipulado en el Dominio A.9.
- 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, de acuerdo con lo estipulado

en el Dominio A.10.

- Prevenir la ~~perdida~~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 de acuerdo con lo estipulado en el Anexo A.11.2.
- Realizar seguimiento al uso de los recursos, ajustar y proyectar los requisitos de capacidad futra con el fin de asegurar el desempeño requerido del o los sistemas de acuerdo con lo estipulado en el Anexo A.12.1.3.
- Asegurar la información y las instalaciones de procesamiento de información se encuentren protegidas contra código malicioso de acuerdo con lo estipulado en el Anexo A.12.2.
- 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, de acuerdo con lo estipulado en el Anexo A.12.3.
- Registrar, conservar y revisar los registros acerca de actividades del usuario para generar evidencias de excepciones, fallas y eventos de seguridad de la información de acuerdo con lo estipulado en el Anexo A.12.4.
- Implementar procedimientos para controlar la instalación Software Operacional en los sistemas operativos de acuerdo con lo estipulado en el Anexo A.12.5.1.
- Prevenir el aprovechamiento de cualquier vulnerabilidad técnica que se pueda presentar mediante la gestión de la vulnerabilidad técnica de acuerdo con lo estipulado en el Anexo A.12.6.
- Planificar y acordar cuidadosamente auditorías que involucren la verificación de los sistemas operativos de acuerdo con lo estipulado en el Anexo A.12.7.
- Asegurar la protección de la información en las redes, sus instalaciones de proceso, protegiéndola al ser transferida mediante cualquier medio de acuerdo con lo estipulado en el Anexo A.13.

Gestión de Talento Humano

- Implementar políticas de aseguramiento a la información que se acceda a través del teletrabajo de acuerdo con lo estipulado en el Anexo A.6.2.2.
- Procurar el cumplimiento, la verificación de requisitos y debida capacitación de los funcionarios que realicen trabajo en casa o teletrabajo tomando conciencia de sus responsabilidades en la protección de la información y las cumplan de acuerdo con lo estipulado en el Dominio A.7.

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 acuerdo con lo

estipulado en el Dominio A.7.

- Definir y documentar junto con los responsables de la información, acuerdos sobre transferencia segura de información, de acuerdo con lo estipulado en el Anexo A.13.2.2.
- 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, de acuerdo con lo estipulado en el Anexo A.13.2.4.
- 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, de acuerdo con lo estipulado en el Anexo A.15.

Oficina Asesora de Planeación

- Definir y asignar las responsabilidades para la seguridad de la información de acuerdo con lo estipulado en el A.6.1.1
- 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 de acuerdo con lo estipulado en el Anexo A. 6.1.5.
- Apoyar la identificación de los activos de información de INVIMA y la definición de las responsabilidades de protección apropiadas, de acuerdo con lo estipulado en el Anexo A.8.
- 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 de acuerdo con lo estipulado en el Anexo A.12.1.2.
- 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, de acuerdo con lo estipulado en el Anexo A.17.
- 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, de acuerdo con lo estipulado en A.18.1.4

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 de acuerdo con lo estipulado en el Anexo A.8.1.4.
- Prevenir el acceso físico no autorizado a las áreas identificadas como críticas por la información que contienen, administran o generan, de acuerdo con lo estipulado en el Anexo A.11.

- 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, de acuerdo con lo estipulado en el Anexo A.15.

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, de acuerdo con lo estipulado en el Anexo A.8.
- 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, de acuerdo con lo estipulado en el Anexo A.8.3.3.

Oficina Asesora Jurídica

- Definir y documentar junto con los responsables de la información, acuerdos sobre transferencia segura de información, de acuerdo con lo estipulado en el Anexo A.13.2.2.
- 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, de acuerdo con lo estipulado en el Anexo A.13.2.4.
- Asesorar con el fin de evitar el incumpliendo en las obligaciones legales o contractuales relacionadas con la seguridad de la información, de acuerdo con lo estipulado en el Anexo A.18.

Oficina de Control Interno

- Apoyar en la revisión Independiente de la seguridad de la Información (Contratar un externo para auditorías internas) de acuerdo con lo estipulado en el Anexo A.18.2.1.
- Formar Auditores Internos en NTC ISO 27001:2013

Grupo de Control Disciplinario Interno

- Incluir dentro del proceso normal las violaciones a la seguridad de la información, de acuerdo con lo estipulado en el Anexo A.7.2.3.

Procesos y Áreas (Servidores Públicos, Contratistas y Proveedores)

- Cumplir con lo definido en las políticas y directrices de protección de la información, de acuerdo con lo estipulado en el Dominio A.5
- Informar a Talento Humano sobre terminación o cambios de responsabilidades de los funcionarios, de acuerdo con lo estipulado en el Anexo A.7.3.1
- Identificar clasificar y valorar los activos de información, de acuerdo con lo estipulado en el Dominio A.8
- Controlar el acceso a la información, apoyándose con TI, Administrativa, talento humano y contractual de acuerdo con lo estipulado en el Dominio A.9.
- 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, de acuerdo con lo estipulado en el Anexo A.12.3.
- Reportar eventos o incidentes de seguridad de la información que evidencies fallas, accesos no autorizados o pérdida de información, de acuerdo con lo estipulado en el Anexo A.16.1.2.
- Identificar la información que contiene datos personales, teniendo en cuenta la ley 1581 y de acuerdo con lo estipulado en el Anexo A.18.1.4.

Oficial de Seguridad de la Información

- Apoyar a INVIMA en la planificación, diseño implementación, operación, revisión y mejora continua de los planes de tratamiento de riesgos de seguridad de la información.
- Apoyar a 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 a 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) de 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 en Línea.
- 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 la misma 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.

Comité de Seguridad de la Información - (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.

10 CRONOGRAMA

De acuerdo con las actividades definidas se presenta el cronograma con vigencia al 2022

Nombre Fase 1: Socialización y planificación	Fecha de Inicio DD/MM/AAAA	Fecha de Fin DD/MM/AAAA	Entregables	$	-
Presentación de proyecto a Comité Institucional de Gestión y Desempeño, para aprobación de proyecto de implementación de Sistema de Gestión de Seguridad de la Información -SGSI.	12/12/2020	12/12/2020	Dcoumentación existente del SGSI, presentación power point y Acta		
Asumir compromiso por parte del Invima para continuar con la implementación y certificación de SGSI.	12/12/2020	12/12/2020	Acta		
Divulgación a nivel institucional del compromiso adquirido de implementación y certificación de SGSI	12/12/2020	31/12/2021	Campaña de comunicaciones		
Generación de ajustes a la documentación al interior de los procesos y planes operativos de la entidad para cumplir con la implementación y certificación de SGSI	1/03/2021	30/09/2021	Documentación revisada y actualizada		
Socialización de avances al comité Institucional de Gestión y Desempeño del presente Proyecto y sus Objetivos	12/12/2020	31/12/2021	Actas		
Diagnosticar y Analizar de la situación de la entidad frente a Seguridad de la información	3/05/2020	4/05/2020	Documentos de autodiagnóstico (FURAG, MSPI, MIPG)		
Planificación de Implementación de SGSI	12/12/2020	31/01/2021	Documento Plan del SGSI		
Nombre Fase 2: Implementación de SGSI	**Fecha de Inicio DD/MM/AAAA**	**Fecha de Fin DD/MM/AAAA**	Entregables	$	-
Creación del proceso SGSI	1/03/2021	30/06/2021	Proceso credo en el mapa de procesos		
Documentación de Procedimientos e instructivos requeridos para la implementación de SGSI.	12/12/2020	1/03/2021	Documentos diseñados para el SGSI		
Nombre Fase 3: Revisión independiente de la seguridad de la información	**Fecha de Inicio DD/MM/AAAA**	**Fecha de Fin DD/MM/AAAA**	Entregables	$	80.000.000,00
Revisión del cumplimiento técnico	1/05/2021	31/09/2021	Informes de resultados de la revisión técnica (Ethical hacking y pruebas de vulnerabilidad e ingeniería social)	$	60.000.000,00
Auditoría interna del SGSI	1/09/2021	30/09/2021	Informe de Auditoría	$	20.000.000,00
Implementación de Mejoras	1/10/2021	28/02/2022	Acciones de mejora implementadas y documentadas (Presupuesto de soporte tecnológico y tecnologías de la información)		
Socialización de resultados a la comité Institucional de Gestión y Desempeño	5/03/2022	20/03/2022	Acta		
Nombre Fase 4:	**Fecha de Inicio DD/MM/AAAA**	**Fecha de Fin DD/MM/AAAA**	Entregables	$	40.000.000,00
Solicitud de certficación	15/04/2022	15/04/2022	Documentación pertinente		
Certificación de SGSI implementado	1/06/2022	30/06/2022	Certificado del ente certificador	$	40.000.000,00

11 PLANES GENERALES DE COMPRAS QUE DESAGREGUEN LOS RECURSOS ASOCIADOS A TODAS LAS FUENTES DE FINANCIACIÓN

Dentro de los planes de adquisiciones se encuentran los siguientes temas:

- Dentro del proyecto Fortalecimiento de la arquitectura tecnológica y los procesos asociados a la gestión de las tecnologías de la información y comunicaciones nacional incluye el ethical hacking

- Curso de formación para auditores internos
- Curso formación personal en temas de seguridad de la información y protección de datos personales
- Plan de adquisiciones para copias de seguridad
- Contratación de contratista que ejerce funciones de Oficial de Seguridad de la Información

12 DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS DE INVERSIÓN

La distribución presupuestal de los proyectos de inversión es la siguiente:

Nombre Fase 3: Revisión independiente de la seguridad de la información	Fecha de Inicio DD/MM/AAAA	Fecha de Fin DD/MM/AAAA	Entregables	$	80.000.000,00
Revisión del cumplimiento técnico	1/05/2021	31/09/2021	Informes de resultados de la revisión técnica (Ethical hacking y pruebas de vulnerabilidad e ingeniería social)	$	60.000.000,00
Auditoría interna del SGSI	1/09/2021	30/09/2021	Informe de Auditoría	$	20.000.000,00
Implementación de Mejoras	1/10/2021	28/02/2022	Acciones de mejora implementadas y documentadas (Presupuesto de soporte tecnológico y tecnologías de la información)		
Socialización de resultados a la comité Institucional de Gestión y Desempeño	5/03/2022	20/03/2022	Acta		
Nombre Fase 4:	**Fecha de Inicio DD/MM/AAAA**	**Fecha de Fin DD/MM/AAAA**	**Entregables**	**$**	**40.000.000,00**
Solicitud de certficación	15/04/2022	15/04/2022	Documentación pertinente		
Certificación de SGSI implementado	1/06/2022	30/06/2022	Certificado del ente certificador	$	40.000.000,00

13 INDICADORES

Nombre del Indicador 1	Incidencia de la socialización y sensibilización en temas de Seguridad de la Información	Fórmula	# de incidentes reportados en el presente año / # de incidentes reportados en el año inmediatamente anterior
Nombre del Indicador 2	Tiempo de respuesta en el tratamiento de incidentes de seguridad de la información	Fórmula	# incidentes presentados / Tiempo promedio transcurrido para la gestión del incidente o evento
Nombre del Indicador 3	Sistema de Gestión Certificado	Fórmula	Sistema de Gestión Certificado

14 MAPAS DE RIESGOS

SECCIÓN 4. RIESGOS	
DESCRIPCION DEL RIESGO	El no cumplimiento de las acciones de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el instituto y su responsabilidad frente a la protección de datos personales.
CAUSAS	* Mecanismos insuficientes para la gestión de los eventos o incidentes que afecten la integridad, confidencialidad y/o disponibiliad de la informacón de la entidad, ocasionando incumplimiento de requisitos legales, normativos o institucionales. * Disposición de recursos (fisicos, tecnologicos, economicos, humanos) insuficientes para generar acciones efectivas frente a la protección de la información en el Invima. • Demoras en los tiempos de contratación. * Indisponibilidad del talento humano. * Falencias en la comunicación con las partes interesadas. * Incumplimiento de la responsabilidad frente a los datos personales por parte de las áreas o procesos.
CONSECUENCIAS	* Posible materialización de incidentes que afecten la seguridad de la información. • Atraso en la ejecución de las actividades del proyecto * Situaciones que afecten el desarrollo de las etapas posteriores del proyecto de Implementación de Sistema de Gestión de Seguridad de la Información. * Afectación a la imagen institucional. * Procesos sancionatorios, legales, penales. * Inadecuado uso de los datos personales.
TIPO DE RIESGO	Estrategico
PROBABILIDAD DE OCURRENCIA	4 Probable
IMPACTO	Mayor
ZONA DE RIESGO	Extrema

15 REQUERIMIENTO DE PERSONAL

De acuerdo con lo anteriormente descrito se es necesario al menos un profesional especialista en seguridad de la información y con la experiencia requerida para la implementación del sistema en entidades del estado colombiano, además del compromiso de todos los responsables de procesos y personal de la entidad.

Esta(s) persona(s) debe dar respuesta y hacer seguimiento a los eventos de seguridad, incidentes y de ser necesario a la ejecución de posibles contingencias. Así como seguimiento a los planes de acción fruto de las auditorías internas.