PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., enero de 2025

1. Contenido

2. 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.”

3. 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.

4. 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

5. 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 2023.
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.

6. PLANES

Dentro de los planes 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 planes:

CIERRE DE BRECHAS ENCONTRADAS EN LA REVISIÓN TÉCNICA INDEPENDIENTE DEL 2023

Continuar junto con el grupo de soporte tecnológico y la oficina de tecnologías de la información con el seguimiento al plan de acción para la mitigación de todas las vulnerabilidades encontradas en el ejercicio del hacking ético del 2023.

CREACIÓN HERRAMIENTA DE EVALUACIÓN SGSI VERSION ISO 27001:2022

De acuerdo con los cambios que se presentaron en la actualización de la norma ISO 27001 Generar una herramienta que permita evaluar la madurez, la implementación de los controles y el cumplimiento de la entidad con respecto a los requisitos de norma y los controles definidos.

Esta herramienta será aplicada como herramienta de evaluación y seguimiento del sistema de gestión de seguridad de la información. que a su vez permitirá cumplir con los requerimientos estipulados por el DAFP, FURAG y el Modelo de Privacidad y seguridad de la información MPSI.

REVISIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de continuar con el ejercicio ya realizado durante el periodo del

2023, 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 realizar una auditoría interna al sistema de gestión de seguridad de la información.

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 27001:2022 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).

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 las auditorías realizadas en años anteriores era la relacionada con **la revisión por la dirección**, se plantean 3 revisiones por la dirección en el año de 2025, 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- Socialización de eventos o incidentes de seguridad de la información presentados en la vigencia.
5- Seguimiento a indicadores del SGSI.

Nota: Es importante aclarar que si se presenta la materialización de un incidente, el seguimiento por la dirección será mayor al estipulado en el presente plan

7. 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:

- Servidores públicos y contratistas de la entidad conocen sus responsabilidades frente a la protección y acceso a la información que administran y generan en su cotidianidad.
- 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.

8. ACCIONES

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

Gestión	Actividades	Tareas	Responsable de la Tarea
Activos de Información	Definir y socializar lineamientos para el levantamiento de activos de información	Incluir la metodología e instrumento de levantamiento de activos de información en el proceso SGSI	Oficial de Seguridad de la Información
	Actualización y levantamiento de Activos de Información incluidas bases de datos personales	Socializar la guía de activos de Información	Equipo de información
		Validar activos de información en el instrumento levantado en la vigencia anterior	Responsable de cada área o proceso y facilitador
		Identificar nuevos activos de información en cada dependencia	Responsable de cada área o proceso y facilitador
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Equipo de información

Gestión	Actividades	Tareas	Responsable de la Tarea
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Equipo de información
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	Responsable de cada área o proceso y facilitador
	Publicación de Activos de Información y registros activos de información ley 1712	Validar y aceptar los activos de información para su publicación en transparencia por cada líder de proceso.	Responsable de cada área o proceso y facilitador
		Consolidar el instrumento de activos de Información.	Equipo de información
		Publicar los instrumentos de activos de información consolidado en transparencia	Equipo de información
	Reporte Datos Personales	Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos.	Responsable de cada área o proceso y facilitador
Gestión de Riesgos	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y	Oficial de seguridad de la información y Padrinos

Gestión	Actividades	Tareas	Responsable de la Tarea
		privacidad de la Información en INTEGRA	
	Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Responsable de cada área o proceso y facilitador
	Publicación	Publicación Matriz de riesgos	Planeación
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Planeación
Gestión de Incidentes de Seguridad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Revisión, actualización y publicación del procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035.	Oficial de Seguridad de la Información
		Socializar el procedimiento a los especialistas de la mesa de	Oficial de Seguridad de la Información

Gestión	Actividades	Tareas	Responsable de la Tarea
		servicio, indicando los cambios en el procedimiento	
		Socializar el procedimiento a los colabores de la Entidad.	Oficial de Seguridad de la Información
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Oficial de Seguridad de la Información
	COLCERT	Socializar los boletines informativos de seguridad, Integrar con COLCERT / Agencia de Ciberseguridad del Gobierno	Oficial de Seguridad de la Información
	Eventos/vulnerabilidades	Realizar seguimiento a los eventos y vulnerabilidades asociados a SGSI	Oficial de Seguridad de la Información - Soporte Tecnológico - OTI
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información
		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los facilitadores de procesos	Oficial de Seguridad de la Información
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información - Comunicaciones
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información - Comunicaciones
Matriz de verificación de Requisitos Legales de	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficial de Seguridad de la Información - Jurídica

Gestión	Actividades	Tareas	Responsable de la Tarea
Seguridad de la Información	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficial de Seguridad de la Información - Jurídica
Protección de datos personales 27701	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Oficial de Seguridad de la Información - Jurídica
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial de Seguridad de la Información - Jurídica
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oficial de Seguridad de la Información - Jurídica

9. PRODUCTOS

El principal producto del presente plan será el Sistema de Gestión de la Seguridad de la Información en cumplimiento con los requisitos de la norma ISO27001:2022 y el Modelo de Seguridad u Privacidad de la Información.

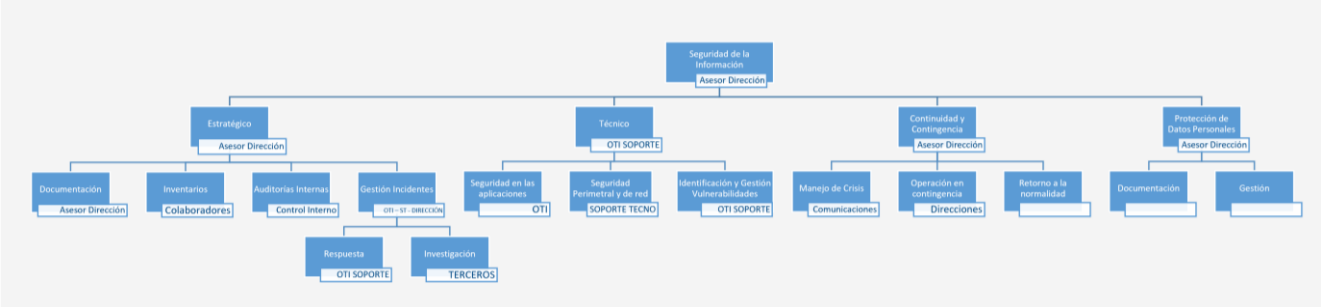
A continuación, se presentan los entregables durante el desarrollo del plan

- Procesos de Seguridad de la Información, documentado e incluido en el mapa de procesos de la Entidad
- Inventario de Activos de Información actualizado
- Riesgos de seguridad de la Información identificados y gestionados
- Gestión de Incidentes de Seguridad de la Información atendidos
- Plan de Cambio y Cultura de Seguridad y Privacidad de la Información
- Matriz de verificación de Requisitos Legales de Seguridad de la Información

- Inventario de Protección de datos personales actualizado

10. RESPONSABLES

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



Además de las responsabilidades específicas ya definidas de acuerdo con lo estipulado en el anexo de la norma ISO 27001:2022.

11. CRONOGRAMA

De acuerdo con las actividades definidas se presenta el cronograma con vigencia al de 2025

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Activos de Información	Definir y socializar lineamientos para el levantamiento de activos de información	Incluir la metodología e instrumento de levantamiento de activos de información en el proceso SGSI	Oficial de Seguridad de la Información	01 de Feb de 2025	18 de Feb de 2025
	Actualización y levantamiento de Activos de Información incluidas bases de datos personales	Socializar la guía de activos de Información	Equipo de información	15 de Feb de 2025	15 de marzo de 2025
		Validar activos de información en el instrumento levantado en la vigencia anterior	Responsable de cada área o proceso y facilitador	15 de marzo de 2025	30 de junio de 2025
		Identificar nuevos activos de información en cada dependencia	Responsable de cada área o proceso y facilitador	15 de marzo de 2025	30 de junio de 2025
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Equipo de información	15 de marzo de 2025	30 de junio de 2025
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Equipo de información	15 de marzo de 2025	30 de junio de 2025
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya	Responsable de cada área o proceso y facilitador	01 de julio de 2025	30 de agosto de 2025

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		inventariados, Materialización de riesgos que cambien la criticidad del activo.			
	Publicación de Activos de Información y registros activos de información ley 1712	Validar y aceptar los activos de información para su publicación en transparencia por cada líder de proceso.	Responsable de cada área o proceso y facilitador	01 de sept de 2025	15 de sept de 2025
		Consolidar el instrumento de activos de Información.	Equipo de información	15 de sept de 2025	30 de sept de 2025
		Publicar los instrumentos de activos de información consolidado en transparencia	Equipo de información	1 oct de 2025	15 de dic de 2025
	Reporte Datos Personales	Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos.	Responsable de cada área o proceso y facilitador	01 de sept de 2025	15 de dic de 2025
Gestión de Riesgos	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información en INTEGRA	Oficial de seguridad de la información y Padrinos	01 de Feb de 2025	30 de marzo de 2025
	Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos	01 de Feb de 2025	30 de dic de 2025

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos	01 de Feb de 2025	30 de dic de 2025
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Responsable de cada área o proceso y facilitador	01 de Feb de 2025	30 de dic de 2025
	Publicación	Publicación Matriz de riesgos	Planeación	01 de Feb de 2025	30 de dic de 2025
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos	01 de jun de 2025	30 de dic de 2025
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos	01 de jun de 2025	30 de agosto de 2025
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la	30 de agosto de 2025	30 de nov de 2025

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
			información y Padrinos		
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Planeación	30 de nov de 2025	15 de dic de 2025
Gestión de Incidentes de Seguridad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Revisión, actualización y publicación del procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035.	Oficial de Seguridad de la Información	24 de enero de 2025	30 de dic de 2025
		Socializar el procedimiento a los especialistas de la mesa de servicio, indicando los cambios en el procedimiento	Oficial de Seguridad de la Información	24 de enero de 2025	30 de dic de 2025
		Socializar el procedimiento a los colabores de la Entidad.	Oficial de Seguridad de la Información	24 de enero de 2025	30 de dic de 2025
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Oficial de Seguridad de la Información	24 de enero de 2025	30 de dic de 2025
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información	24 de enero de 2025	30 de dic de 2025
	Eventos/vulnerabilidades	Realizar seguimiento a los eventos y vulnerabilidades asociados a SGSI	Oficial de Seguridad de la Información - Soporte Tecnológico - OTI	24 de enero de 2025	30 de dic de 2025

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información	24 de enero de 2025	15 de feb de 2025
		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los facilitadores de procesos	Oficial de Seguridad de la Información	15 de Feb de 2025	01 de marzo de 2025
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información - Comunicaciones	01 de marzo de 2025	30 de dic de 2025
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información - Comunicaciones	01 de marzo de 2025	30 de dic de 2025
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficial de Seguridad de la Información - Jurídica	01 de agosto de 2025	30 de sept de 2025
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficial de Seguridad de la Información - Jurídica	01 de agosto de 2025	30 de sept de 2025
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Oficial de Seguridad de la Información - Jurídica	01 de Feb de 2025	15 de marzo de 2025

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial de Seguridad de la Información - Jurídica	15 de marzo de 2025	01 jun de 2025
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oficial de Seguridad de la Información - Jurídica	01 jun de 2025	30 de jul de 2025

12. 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 plan 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

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.

Este profesional debe contar con el apoyo de al menos dos personas con conocimientos en seguridad en las operaciones, Seguridad perimetral y de red.

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.