

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**Bogotá D.C., 26 enero de
2026**

Contenido

1	ALCANCE DEL PLAN	3
2	OBJETIVO	3
3	OBJETIVOS ESPECÍFICOS	3
4	ESTRATEGIAS	3
5	PLANES	4
5.1	CIERRE DE BRECHAS ENCONTRADAS EN LAS REVISIONES TÉCNICAS INDEPENDIENTES	5
5.2	EVALUAR EL GRADO DE MADUREZ DEL SGSI BAJO LA NORMA NTC ISO/IEC 27001:2022	5
5.3	REVISIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	5
5.4	REVISIÓN POR LA DIRECCIÓN DEL AVANCE DEL PLAN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	5
6	METAS	6
7	ACCIONES	6
8	PRODUCTOS	10
9	RESPONSABLES	11
10	CRONOGRAMA	11
11	PLANES GENERALES DE COMPRAS QUE DESAGREGUEN LOS RECURSOS ASOCIADOS A TODAS LAS FUENTES DE FINANCIACIÓN	17
12	INDICADORES	17
13	MAPAS DE RIESGOS	17
14	REQUERIMIENTO DE PERSONAL	18

1 ALCANCE DEL PLAN

La planificación, implementación, gestión, operación y mejoramiento continuo 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, siguiendo los lineamientos del Sistema Integrado de Procesos institucional lo que incluye, las actividades de revisión, formalización y socialización de las políticas técnicas, procesos, procedimientos, controles y demás documentación que permite al SGSI un trabajo articulado con el Sistema de Gestión Integrado – SGI donde se manifiesta lo siguiente:

“El Invima diseña, promueve y adopta 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

El plan de seguridad y privacidad tiene como objetivo determinar, ejecutar y evaluar las acciones que se realizarán durante la vigencia 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, frente a amenazas potenciales y reales que puedan afectar su confidencialidad, integridad, disponibilidad y privacidad.

3 OBJETIVOS ESPECÍFICOS

- Revisar, actualizar los riesgos de seguridad de la información.
- Implementar y operar los controles seleccionados para el tratamiento de los riesgos.
- Mejorar las capacidades de respuesta del Instituto frente a eventos de seguridad con acciones de sensibilización en seguridad informática.
- Actualizar la documentación que soporta el SGSI.
- Evaluar la efectividad de las acciones de control de riesgo.
- Identificar y resolver brechas de seguridad en los activos de información.
- Aplicar procesos de evaluación independiente para mejorar el desempeño de la seguridad informática.

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- Fortalecer el SGSI del instituto a través de la adopción de nuevos procedimientos y controles gestionables y efectivos dentro del marco del Sistema Integrado de Gestión del Instituto
- 2- Sensibilizar a las diferentes áreas y procesos de la entidad sobre las responsabilidades que tienen frente a la protección y acceso a la información y como puede contribuir a la mejora de la misma.
- 3- 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.
- 4- Implementar acciones que permitan cerrar brechas de seguridad en los diferentes activos del Instituto
- 5- Actualizar la documentación del SGSI siguiendo los marcos de referencia recomendados por las normativas vigentes en materia de seguridad de la información.

5 PLANES

Dentro de los planes establecidos para seguridad de la información se encuentran:

- a) Aprovechar las herramientas documentales del sistema integrado de gestión para controlar la producción y socialización de la documentación que apoya el SGSI
- b) Realizar pruebas de análisis de vulnerabilidades y Ethical hacking sobre la infraestructura tecnológica del Instituto a través de los servicios del C-SIRT Salud
Evaluar la brecha existente entre los requisitos de la Norma NTC ISO/IEC 27001:2022 “Sistemas de gestión de seguridad de la información y el SGSI del Instituto para identificar y planificar acciones de mejora.

Los anteriores planes se complementan con las siguientes acciones específicas:

5.1 CIERRE DE BRECHAS ENCONTRADAS EN LAS REVISIONES TÉCNICAS INDEPENDIENTES

Usando las capacidades del grupo de soporte tecnológico y la oficina de tecnologías de la información mantener actividades de diagnóstico y cierre de vulnerabilidades sobre la infraestructura tecnológica realizando aplicación periódica de parches de seguridad, actualizado sistemas operacionales, implementando controles compensatorios y evaluando la pertinencia de uso de dispositivos informáticos con brechas de seguridad.

5.2 EVALUAR EL GRADO DE MADUREZ DEL SGSI BAJO LA NORMA NTC ISO/IEC 27001:2022

Usando recursos propios se propone evaluar el estado de madurez actual del SGSI del Instituto frente a los nuevos requisitos del Modelo de Seguridad y Privacidad de MINTIC y la versión actualizada norma NTC ISO/IEC 27001.

Usar los resultados de la evaluación de madurez del SGSI para definir acciones de mejoramiento y reportar los avances en la gestión de la seguridad de la información en las evaluaciones requeridas por el DAFP en el FURAG y el Modelo de Privacidad y seguridad de la información -MPSI MINTIC.

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

Mantener las acciones de evaluación independiente del SGSI realizadas en las vigencias previas para identificar procedimientos, controles y actividades susceptibles de mejora o con debilidades que requieren tratamiento inmediato.

Evaluar de manera independiente usando técnicas de auditoria el estado de cumplimiento del SGSI frente a sus requisitos internos y las obligaciones normativas en materia de seguridad de la información.

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

Utilizar las herramientas de seguimiento y control del sistema integrado de gestión institucional para que la Dirección del Instituto conozca de primera mano el estado y beneficios alcanzados por las acciones de gestión de seguridad de la información mediante:

- 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

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:

- 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.

7 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
	Actualizar el 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	Equipo de información

Gestión	Actividades	Tareas	Responsable de la Tarea
		realimentar a las áreas con las modificaciones.	
		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
	Responder a eventos de seguridad	Aplicar las acciones de tratamiento de riesgos a los eventos de seguridad identificados	Oficial de Seguridad de la Información
	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

Gestión	Actividades	Tareas	Responsable de la Tarea
		Socializar el procedimiento a los especialistas de la mesa de servicio, indicando los cambios en el procedimiento	Oficial de Seguridad de la Información
		Socializar el procedimiento a los colaboradores 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 con 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
	C SIRT SALUD	Apoyar la ejecución de análisis de vulnerabilidades y detección de amenazas potenciales sobre la infraestructura del instituto	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 Sensibilización y mejoramiento de la Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el Plan de Sensibilización y mejora de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información
		Publicar y Socializar el Plan de Sensibilización y mejora de Cultura Organizacional en Apropiación del SGSI con los facilitadores de procesos	Oficial de Seguridad de la Información
	Ejecutar el Plan de Sensibilización y mejoramiento de la 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

Gestión	Actividades	Tareas	Responsable de la Tarea
	Evaluar los resultados de la ejecución del Plan de Sensibilización y mejoramiento de la 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 Seguridad de la Información	Actualizar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Identificar y aplicar cambios sobre la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficial de Seguridad de la Información - Jurídica
	Revisión del nivel de cumplimiento de los Requisitos Legales de Seguridad de la Información	Recolectar las evidencias de cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficial de Seguridad de la Información - Jurídica
Protección de datos personales 27701	Identificar nuevas bases de datos con información personal en uso en el Instituto	Elaborar y emitir un memorando para la actualización del inventario de bases de datos personales de acuerdo con los estándares emitidos por la SIC (Superintendencia de Industria y Comercio)	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

8 PRODUCTOS

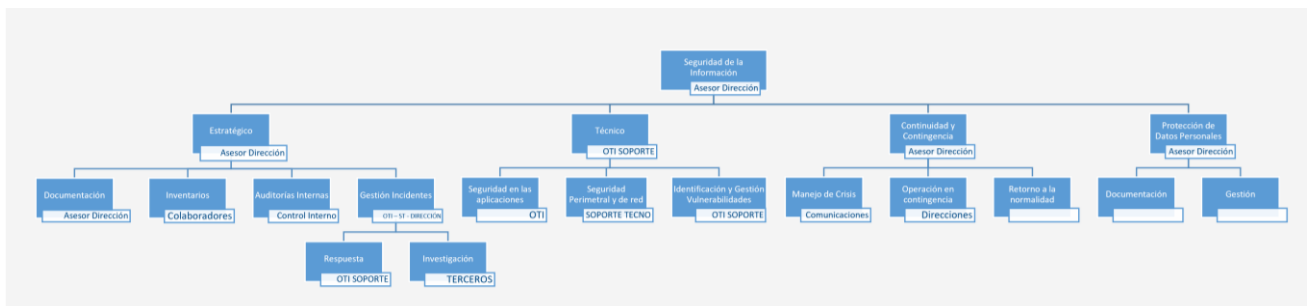
El principal producto del presente plan será el Sistema de Gestión de la Seguridad de la Información en cumplimiento con los requisitos de la norma ISO27001:2022 y el Modelo de Seguridad y Privacidad de la Información.

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

- Procesos de Seguridad de la Información, documentados e incluidos en el mapa de procesos de la Entidad.
- Inventario de Activos de Información actualizado.
- Riesgos de seguridad de la Información identificados y gestionados.
- Incidentes de Seguridad de la Información adecuadamente gestionados.
- Plan de Sensibilización y mejoramiento de la Cultura de Seguridad y Privacidad de la Información y Seguridad Digital ejecutado.
- Matriz de verificación de Requisitos Legales de Seguridad de la Información actualizado.
- Inventario de Protección de datos personales actualizado.

9 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.

10 CRONOGRAMA

De acuerdo con las actividades definidas se presenta el cronograma con vigencia al de 2026

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 2026	18 de Feb de 2026
	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 2026	15 de marzo de 2026
		Validar activos de información en el instrumento levantado en la vigencia anterior	Responsable de cada área o proceso y facilitador	15 de marzo de 2026	30 de junio de 2026
		Identificar nuevos activos de información en cada dependencia	Responsable de cada área o proceso y facilitador	15 de marzo de 2026	30 de junio de 2026
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Equipo de información	15 de marzo de 2026	30 de junio de 2026
		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 2026	30 de junio de 2026
		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,	Responsable de cada área o proceso y facilitador	01 de julio de 2026	30 de agosto de 2026

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	Publicación de Activos de Información y registros activos de información ley 1712	Materialización de riesgos que cambien la criticidad del activo.			
		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 2026	15 de sept de 2026
		Consolidar el instrumento de activos de Información.	Equipo de información	15 de sept de 2026	30 de sept de 2026
		Publicar los instrumentos de activos de información consolidado en transparencia	Equipo de información	1 oct de 2026	15 de dic de 2026
	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 2026	15 de dic de 2026
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 2026	30 de marzo de 2026
	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 2026	30 de dic de 2026

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 2026	30 de dic de 2026
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Responsable de cada área o proceso y facilitador	01 de Feb de 2026	30 de dic de 2026
	Publicación	Publicación Matriz de riesgos	Planeación	01 de Feb de 2026	30 de dic de 2026
	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 2026	30 de dic de 2026
	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 2026	30 de ago de 2026
	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	30 de agosto de 2026	30 de nov de 2026
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Planeación	30 de nov de 2026	15 de dic de 2026

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
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	14 de febrero de 2026	30 de mar de 2026
		Socializar el procedimiento a los especialistas de la mesa de servicio, indicando los cambios en el procedimiento	Oficial de Seguridad de la Información	1 de marzo de 2026	30 de mar de 2026
		Socializar el procedimiento a los colaboradores de la Entidad.	Oficial de Seguridad de la Información	1 de marzo de 2026	30 de mar de 2026
	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	1 de marzo de 2026	30 de dic de 2026
	CSIRT-SALUD	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información	24 de enero de 2026	30 de dic de 2026
	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 2026	30 de dic de 2026
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	20 de febrero de 2026	25 de feb de 2026
		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	25 de Feb de 2026	01 de marzo de 2026

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	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 2026	30 de dic de 2026
	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 abril de 2026	30 de dic de 2026
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 mayo de 2026	30 de sept de 2026
	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	30 de mayo de 2026	30 de sept de 2026
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 2026	15 de marzo de 2026
	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 2026	01 jun de 2026
	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 2026	30 de jul de 2026

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:

- Plan de adquisiciones para copias de seguridad
- Contratación de profesional que apoya la gestión de la Seguridad de la Información

ELEMENTOS	FUENTE	VALOR	OBSERVACIONES
Profesional Especializado en Seguridad Informática	Inversión	\$ 99.759.000	Contratista

12 INDICADORES

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

13 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 disponibilidad de la información de la entidad, ocasionando incumplimiento de requisitos legales, normativos o institucionales. * Disposición de recursos (físicos, tecnológicos, económicos, 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	Estratégico
PROBABILIDAD DE OCURRENCIA	4 Probable
IMPACTO	Mayor
ZONA DE RIESGO	Extrema

14 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 fruto de las auditorías internas.