PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., Enero 26 de 2026

CONTENIDO

1. ALCANCE

Teniendo en cuenta que el modelo integrado de planeación y gestión (MIPG) integra el sistema de gestión de calidad y el desarrollo administrativo, así como el cumplimiento de los requisitos que incluyen los riesgos que puedan afectar a cualquier activo de información en cuanto a confidencialidad, integridad , disponibilidad y privacidad el presente plan aplica para todos los riesgos de seguridad de la información identificados en el Instituto que puedan afectar a uno o más procesos del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información y el plan de Seguridad y Privacidad de la información establecido para la vigencia 2026.

2. OBJETIVO

Aplicar la Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información en la herramienta del sistema de gestión integrado para identificar, implementar, mantener y mejorar los controles de seguridad de la información necesarios para mitigar la materialización de los riesgos de seguridad de la información en el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA.

3. OBJETIVOS ESPECÍFICOS

- Actualizar el inventario de activos de información que soportan los procesos del instituto
- Identificar amenazas y vulnerabilidades puedan afectar el desarrollo de las actividades realizadas por e Invima o sus activos de información.
- Socializar la Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, a todas las áreas y procesos con el fin de gestionar de manera efectiva los riesgos que afectan la protección de la información en el Instituto.
- Identificar mecanismos de control que permitan a todos los procesos del Instituto la definición y seguimiento de los riesgos de seguridad de la información, así como identificar las responsabilidades frente a acciones y controles de mitigación de riesgos en el Invima.
- Identificar acciones de mejora para cada control que requiera fortalecimiento teniendo en cuenta los lineamientos existentes para la gestión de riesgos.
- Aplicar los planes de tratamiento de riesgos seleccionados para prevenir la materialización de eventos de riesgo de seguridad de la información.
- Evaluar el desempeño y efectividad de los controles seleccionados para el tratamiento de los riesgos de seguridad digital.
- Responder en forma efectiva a los eventos de riesgo si los mismos se materializan.
- Facilitar el monitoreo y revisión de las responsabilidades y ejecución de las actividades relacionadas a los controles definidos o para la mejora de éstos en miras a la mitigación de los riesgos identificados.

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 el tratamiento de los riesgos de seguridad de la información identificados:

1. Sensibilizar a las diferentes áreas y procesos de la entidad sobre la importancia de identificar los activos de información, su valor tanto para el proceso como para la entidad y los mecanismos que se tienen para proteger la información en cuanto a confidencialidad integridad, disponibilidad y disponibilidad.
2. Generar alianzas entre procesos de apoyo que administren y gestionen controles que permitan proteger la información del Invima.
3. Implementar acciones que permitan trabajar en equipos interdisciplinarios generando sinergias entre los diferentes procesos para proteger la información.
4. Aprovechar los servicios del C-SIRT Salud para identificar amenazas y vulnerabilidades sobre los activos de información institucionales.
5. Implementar controles de seguridad que permitan la mitigación de los riesgos de seguridad de la información identificados.

5. PROYECTOS

Con el fin de prevenir la materialización de las amenazas que pueden afectar la disponibilidad confidencialidad, integridad y privacidad de la información del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, se presenta a continuación los planes o proyectos definidos para la identificación de los riesgos y su seguimiento.

- Realizar talleres junto con la oficina asesora de planeación para la identificación de riesgos de seguridad de la información que puedan afectar los activos de información del Invima en todas las áreas y procesos.

- Identificar requerimientos técnicos y tecnológicos que apoyen la protección de la información confidencial de la institución.
- Seleccionar, implementar y gestionar los controles de seguridad más adecuados que faciliten al instituto la protección de sus activos frente a las amenazas reales o potenciales
- Realizar sesiones de sensibilización que permiten la apropiación efectiva del sistema de gestión de seguridad de la información, sus controles y las responsabilidades que cada uno de los servidores públicos, contratistas o proveedores tienen sobre la información que administran generan o conservan.

6. METAS

Dentro de las metas propuestas en la ejecución del plan de tratamiento de riesgos de seguridad de la información del Invima, se proponen las siguientes:

- Trabajar de forma conjunta con todas las áreas y procesos del Instituto con el fin de mitigar los riesgos identificados en la entidad.
- Gestionar adecuadamente los riesgos de seguridad de la información haciendo uso de los mecanismos y herramientas existentes en la entidad y basados en la guía de identificación y administración de riesgos dada por el DAFP.
- Mejoras de controles definidos con el fin de ser fortalecidos y socializados con todas las partes interesadas.
- Generar conciencia de las responsabilidades que cada miembro del equipo de trabajo del Invima tiene frente la gestión de los riesgos de seguridad de la información ya sea ésta de forma digital, impresa o por gestión del conocimiento.

7. ACCIONES

Verificar posibles actualizaciones sobre la Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información en INTEGRA de acuerdo con las modificaciones formuladas por el DAFP a la guía de administración y gestión de riesgos.

Realizar reuniones con los diferentes equipos de trabajo para la identificación de los riesgos de seguridad de la información y sus respectivos seguimientos.

Se presentan de forma general las acciones a realizar:

Gestión	Actividades
Gestión de Riesgos	Sensibilización sobre la Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información en INTEGRA
	Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital

Gestión	Actividades
	Aceptación de Riesgos Identificados por el comité directivo
	Publicación de la matriz de riesgos de seguridad digital
	Seguimiento a la Fase de Tratamiento de los riesgos de seguridad digital
	Evaluación de riesgos residuales
	Mejoramiento de controles de seguridad
	Monitoreo y Revisión de la efectividad de los planes de tratamiento de riesgos
Gestión de Incidentes de Seguridad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información
	Gestionar los incidentes de Seguridad de la Información identificados
	COLCERT / C SIRT SALUD
	Eventos/Incidentes

8. PRODUCTOS

Dentro de los productos que se deben generar para el tratamiento de riesgos de seguridad de la información se encuentran: Los riesgos de seguridad de la información identificados y valorados, evidencias del seguimiento y gestión de riesgos, seguimiento a planes de acción.

Gestión	Actividades	Tareas
Gestión de Riesgos	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y 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
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento
	Publicación	Publicación Matriz de riesgos
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias
	Evaluación de riesgos residuales	Evaluación de riesgos residuales
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores

Gestión	Actividades	Tareas
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.
		Socializar el procedimiento a los especialistas de la mesa de servicio, indicando los cambios en el procedimiento
		Socializar el procedimiento a los colabores de la Entidad.
	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.
	COLCERT / Agencia Nacional de Seguridad Digital	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno
	Eventos/ Incidentes	Realizar seguimiento a los eventos y vulnerabilidades asociados a SGSI

9. RESPONSABLES

Todas las áreas y procesos del Instituto Nacional de Vigilancia de Medicamen
tos y Alimentos INVIMA, son responsables de la identificación, aplicación de controles y tratamiento de riesgos de seguridad de la información identificados en la entidad.

Gestión	Actividades	Tareas	Responsable de la Tarea
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
	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

Gestión	Actividades	Tareas	Responsable de la Tarea
	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 servicio, indicando los cambios en el procedimiento	Oficial de Seguridad de la Información
		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
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de 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

10. CRONOGRAMA

Cada control cuenta con su responsable definido de acuerdo con la autoridad que este tiene y las funciones asignadas por su cargo

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
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	15 de Feb de 2026	30 de marzo de 2026

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	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	15 de Feb de 2026	30 de diciembre de 2026
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos	15 de Feb de 2026	30 de diciembre de 2026
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Responsable de cada área o proceso y facilitador	15 de Feb de 2026	30 de diciembre de 2026
	Publicación	Publicación Matriz de riesgos	Planeación	15 de Feb de 2026	30 de diciembre 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 marzo 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 marzo 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 marzo de 2026
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Planeación	30 de nov de 2026	30 de marzo de 2026
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 colabores 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	Oficial de Seguridad de la Información	1 de marzo de 2026	30 de dic de 2026

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		de acuerdo a lo establecido en el procedimiento definido.			
	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

11. PLANES GENERALES DE COMPRAS

Dentro de los planes presupuestados para ayudar con la mitigación de los riesgos de seguridad de la información y la identificación de los mismos en el periodo del de 2026 se proponen los siguientes temas relacionados:

1- Plan de adquisiciones de la oficina de tecnologías de la información y el grupo de soporte tecnológico vistas y apoyadas con seguridad de la información.
2- Plan proyecto fortalecimiento desde planeación para toda la entidad
   a. Servicio ***de* cacería de amenazas (threat hunting)**: *"…el proceso de búsqueda iterativa y proactiva a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes*." en equipos de usuario final incluidos servidores.

   b. Análisis de Comportamiento:

      1. **Seguridad e-mail cloud**: Servicio de análisis que detiene la suplantación de identidad, los ataques a direcciones de correo empresariales, el ransomware y el correo no deseado; mejorando la seguridad para el correo electrónico de Office 365.

      2. **Servicio de PAM (control de acceso a cuentas con privilegios)**: Ayuda a proteger las organizaciones contra las amenazas cibernética ya que supervisa, detecta y evita el acceso con privilegios no autorizado a recursos críticos.

   c. **Servicio de Monitoreo de Directorio Activo:** supervisa las métricas de rendimiento críticas y realiza importantes pruebas de diagnóstico. También identifica los cuellos de botella en el rendimiento e implementa acciones correctivas para resolverlos, asegurando el buen funcionamiento de los servicios del Directorio Activo.

   d. **Gestión de vulnerabilidades**: El objetivo principal de la gestión de vulnerabilidades es reducir el riesgo de una posible explotación de vulnerabilidades técnicas y proteger los activos

críticos de la organización. A través de la identificación, clasificación, priorización y mitigación de estas en los sistemas y aplicaciones.

e. **Respuesta a incidentes:** Planificación, preparación y respuesta a incidentes de seguridad, incluyendo la investigación y contención de los incidentes.

12. DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS DE INVERSIÓN

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

ELEMENTOS	FUENTE	VALOR	OBSERVACIONES
Equipos de Seguridad	Inversión	$ 1.999.688.274	Contrato de Servicios Tecnológicos Integrados
FireEye - Trellix	Inversión	$ 258.756.596	Contrato de Ciberseguridad
Umbrella (Análisis de DNS - Cisco - EDR)	Inversión	$ 737.093.280	Contrato de Ciberseguridad
Profesional Especializado en Seguridad Informática	Inversión	$ 99.759.000	Contratista
Profesional especialista en Directorio Activo	Inversión	$ 81.449.433	Contratista

Nota: Se hace salvedad qué esta distribución presupuestal puede variar de acuerdo con las necesidades de tratamiento de riesgos de la entidad y que está planteada solo desde seguridad de la información.

La distribución presupuestal dedicada por la OTI para implementaciones de política de Gobierno digital y por soporte tecnológico para la implementación de la realización de sus labores y obligaciones que además pueden incluir temas de seguridad de la información hacen parte de otros planes y otros documentos

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 fruto de las auditorías internas.