MINISTERIO DE SALUD
Y PROTECCIÓN SOCIAL

invima
Instituto Nacional de Vigilancia de Medicamentos y Alimentos.

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

Bogotá D.C., 2023

CONTENIDO

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 y disponibilidad 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.

OBJETIVO

Definir los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información en el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA. Así como el tratamiento de los riesgos de la Seguridad y Privacidad de la Información.

OBJETIVOS ESPECÍFICOS

- Identificar aspectos que pueden afectar el desarrollo de las actividades de mitigación de riesgos del Invima.
- socializar las metodológicas existentes para la gestión de riesgos del Invima 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.
- permitir a través de la definición y seguimiento de los riesgos de seguridad de la información 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.
- 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.

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 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.

PROYECTOS

Con el fin de prevenir la materialización de las amenazas que pueden afectar la disponibilidad confidencialidad o integridad 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.

- Generar una nueva metodología para la gestión de riesgos institucionales, teniendo en cuenta la guía del DAFP y el documento SGI-EMC-PR003 Procedimiento Gestión de Riesgos Institucionales, con le que cuenta la entidad.
- Realizar talleres junto con la oficina asesora de planeación para la identificación de riesgos del Invima con todas las áreas y procesos.
- Identificar requerimientos técnicos y tecnológicos que apoyen la protección de la información confidencial de la institución.
- 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

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:

- Trabajo de forma conjunta con todas las áreas y procesos del Instituto Con el fin de mitigar los riesgos identificados en la entidad.
- Riesgos de seguridad de la información gestionados de forma efectiva 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.

ACCIONES

De acuerdo con la guia del DAFP número 5 se realizarán los ajustes necesarios en la herramienta Integra, se realizarán 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
	Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital
	Aceptación de Riesgos Identificados
	Publicación
	Seguimiento Fase de Tratamiento
	Evaluación de riesgos residuales
	Mejoramiento
	Monitoreo y Revisión
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
	CSIRT

Gestión	Actividades
	Eventos/vulnerabilidades

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 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

Gestión	Actividades	Tareas
		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.
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno
	Eventos/vulnerabilidades	Realizar seguimiento a los eventos y vulnerabilidades asociados a SGSI

RESPONSABLES

Todas las áreas y procesos del Instituto Nacional de Vigilancia de Medicamentos 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

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	01 de Feb de 2023	30 de marzo de 2023
	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 2023	30 de marzo de 2023
		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 2023	30 de marzo de 2023
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Responsable de cada área o proceso y facilitador	01 de Feb de 2023	30 de marzo de 2023
	Publicación	Publicación Matriz de riesgos	Planeación	01 de Feb de 2023	30 de marzo de 2023
	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 2023	30 de agost de 2023
	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 2023	30 de agost de 2023
	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 agost de 2023	30 de nov de 2023
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Planeación	30 de nov de 2023	15 de dic de 2023
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 2023	30 de dic de 2023

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		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 2023	30 de dic de 2023
		Socializar el procedimiento a los colabores de la Entidad.	Oficial de Seguridad de la Información	24 de enero de 2023	30 de dic de 2023
	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 2023	30 de dic de 2023
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información	24 de enero de 2023	30 de dic de 2023
	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 2023	30 de dic de 2023

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 2023 se proponen los siguientes temas relacionados:

1- Contratación de una ética al hacking qué comprueben vulnerabilidades internas y de la red en el Invima.
2- 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.
3- Plan proyecto fortalecimiento desde planeación para toda la entidad

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
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

Nota: Se hace salvedad qué esta distribución presupuestal puede variar de acuerdo a 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

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

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 disponibilad 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

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.