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

Bogotá D.C., 2021

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 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.

2. 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.

3. 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.

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 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.

5. 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

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:

- 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.

7. ACCIONES

Las acciones que permiten tratar los riesgos de seguridad de la información se ejecutan teniendo en cuenta dos aspectos fundamentales; el primero son acciones de mejora a los controles que en su valoración de solidez sea débil; la segunda es generar construir o definir nuevos controles que permitan apoyar la mitigación de los riesgos identificados en la entidad.

Para cumplir con estas acciones se presenta a continuación los controles que por su valoración en solidez requieren un plan de mejora:

Control	Plan de mejora / Acciones
Definición de perfiles de Acceso por procesos y áreas	Generar la documentación de perfiles de acceso para cada una de las áreas del Invima. Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, teniendo en cuenta el tiempo de ejecución de contrato para estos últimos. Implementar las directrices de seguridad para el acceso a la información

Control	Plan de mejora / Acciones
Definición y socialización de las rutas digitales para el almacenamiento de la información	Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento. Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por la oficina de tecnología.

Nuevos controles

Control	Plan de mejora / Acciones
Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información.	Realizar pruebas de restauración periódicas junto con el responsable de la información tomando al azar áreas o procesos que hayan identificado activos de información importantes en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo. Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos personales sensibles.
Identificar riesgos de seguridad de la información en todos los proyectos y controles de cambios de la entidad	Tener en cuenta la visión de seguridad de la información la identificación de riesgos para la ejecución de nuevos proyectos dentro de la entidad, no solo para los proyectos de carácter tecnológico. Tener en cuenta el punto de vista de seguridad de la información en los controles de cambios para aplicativos desarrollados interna o externamente en la entidad.
Documentar las acciones realizadas por mesa de ayuda	Sensibilizar a todos los miembros del equipo de soporte tecnológico frente a la importancia de la documentación que se debe tener en cualquiera de las acciones realizadas frente a configuraciones de permisos de acceso a la información, solicitud de borrado de información, entrega de información o actualizaciones a la información.
Mejoras en los procesos y procedimientos qué administren información	Sensibilizar a todo el personal frente a la necesidad de incluir la protección de la información en los procesos o procedimientos que lo requieran. Definir metodologías o mecanismos de anonimización de la información ya sea ésta de forma digital (bases de datos, documentos electrónicos, entre otros) o impresa

8. PRODUCTOS

Dentro de los productos que se deben generar para el tratamiento de riesgos de seguridad de la información se encuentran: implementar las mejoras definidas para los controles existentes que así lo requieran y Generar actividades para los controles nuevos diseñados.

Para cumplir con estas acciones se presenta a continuación Las acciones de mejora su responsable y la evidencia qué se espera:

Control	Plan de mejora / Acciones	Responsable	Evidencia
Definición de perfiles de Acceso por procesos y áreas	Generar la documentación de perfiles de acceso para cada una de las áreas del Invima. Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, teniendo en cuenta el tiempo de ejecución de contrato para estos últimos. Implementar las directrices de seguridad para el acceso a la información	Responsables de las áreas y procesos del Invima. Grupo de Soporte Tecnológico Oficial de seguridad de la información	Listado de perfiles básicos de acceso por cada proceso y área. Configuración el directorio activo de los perfiles identificados seguimientos a la identificación y configuración de perfiles
Definición y socialización de las rutas digitales para el almacenamiento de la información	Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento. Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por la oficina de tecnología.	oficial de seguridad de la información, oficina de tecnologías de la información y grupo de soporte tecnológico.	charlas y comunicados a través de Systemplus sobre rutas digitales de almacenamiento de la información para funcionarios o contratistas.

Nuevos controles

Control	Plan de mejora / Acciones	Responsable	Evidencia
Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información.	Realizar pruebas de restauración periódicas junto con el responsable de la información tomando al azar áreas o procesos que hayan identificado activos de información importantes en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo. Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos personales sensibles.	Grupo soporte tecnológico en conjunto con el propietario de la información o quien éste designe	pruebas de restauración documentadas
Identificar riesgos de seguridad de la información en todos los proyectos y controles de cambios de la entidad	Tener en cuenta la visión de seguridad de la información la identificación de riesgos para la ejecución de nuevos proyectos dentro de la entidad, no solo para los proyectos de carácter tecnológico. Tener en cuenta el punto de vista de seguridad de la información en los controles de cambios para aplicativos desarrollados interna o externamente en la entidad.	Oficinas, áreas y procesos. Oficial de seguridad de la información	Inclusión de la actividad de identificación de riesgos o requerimientos de seguridad de la información. Textos redactados con riesgos identificados, requerimientos y/o conceptos de seguridad de la información frente a las actividades propuestas en los proyectos a realizar o ejecutar
Documentar las acciones realizadas por mesa de ayuda	Sensibilizar a todos los miembros del equipo de soporte tecnológico frente a la importancia de la documentación que se debe tener en cualquiera de las acciones realizadas frente a configuraciones de permisos de acceso a la información, solicitud de borrado de información, entrega de información o actualizaciones a la información.	Grupo soporte tecnológico Oficial de seguridad de la información	Sensibilización y capacitación es sobre cómo documentar las actividades realizadas en mesa de ayuda, con el fin de generar evidencia de quien la solicita porque se solicitan bajo qué parámetros se autorizan las solicitudes todo en el marco de la protección de la información.
Mejoras en los procesos y procedimientos qué administren información	Sensibilizar a todo el personal frente a la necesidad de incluir la protección de la información en los procesos o procedimientos que lo requieran. Definir metodologías o mecanismos de anonimización de la información ya sea ésta de forma digital (bases de datos, documentos electrónicos, entre otros) o impresa	Oficinas, áreas y procesos. Oficial de seguridad de la información	Inclusión en los procesos y procedimientos temas relacionados con la protección de la información de acuerdo a las políticas de seguridad de la información. Identificación de las actividades necesarias para realizar una correcta animación de la información.

9. 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.

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

Control	Plan de mejora / Acciones	Responsable
Definición de perfiles de Acceso por procesos y áreas	Generar la documentación de perfiles de acceso para cada una de las áreas del Invima. Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, teniendo en cuenta el tiempo de ejecución de contrato para estos últimos. Implementar las directrices de seguridad para el acceso a la información	Responsables de las áreas y procesos del Invima. Grupo de Soporte Tecnológico Oficial de seguridad de la información
Definición y socialización de las rutas digitales para el almacenamiento de la información	Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento. Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por la oficina de tecnología.	oficial de seguridad de la información, oficina de tecnologías de la información y grupo de soporte tecnológico.

Nuevos controles

Control	Plan de mejora / Acciones	Responsable
Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información.	Realizar pruebas de restauración periódicas junto con el responsable de la información tomando al azar áreas o procesos que hayan identificado activos de información importantes en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo. Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos personales sensibles.	Grupo soporte tecnológico en conjunto con el propietario de la información o quien éste designe
Identificar riesgos de seguridad de la información en todos los proyectos y controles de cambios de la entidad	Tener en cuenta la visión de seguridad de la información la identificación de riesgos para la ejecución de nuevos proyectos dentro de la entidad, no solo para los proyectos de carácter tecnológico. Tener en cuenta el punto de vista de seguridad de la información en los controles de cambios para aplicativos desarrollados interna o externamente en la entidad.	Oficinas, áreas y procesos. Oficial de seguridad de la información

Control	Plan de mejora / Acciones	Responsable
Documentar las acciones realizadas por mesa de ayuda	Sensibilizar a todos los miembros del equipo de soporte tecnológico frente a la importancia de la documentación que se debe tener en cualquiera de las acciones realizadas frente a configuraciones de permisos de acceso a la información, solicitud de borrado de información, entrega de información o actualizaciones a la información.	Grupo soporte tecnológico Oficial de seguridad de la información
Mejoras en los procesos y procedimientos qué administren información	Sensibilizar a todo el personal frente a la necesidad de incluir la protección de la información en los procesos o procedimientos que lo requieran. Definir metodologías o mecanismos de anonimización de la información ya sea ésta de forma digital (bases de datos, documentos electrónicos, entre otros) o impresa	Oficinas, áreas y procesos. Oficial de seguridad de la información

10. CRONOGRAMA

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

Control	Plan de mejora / Acciones	Responsable	Fechas de implementación	
			Inicio	Fin
Definición de perfiles de Acceso por procesos y áreas	Generar la documentación de perfiles de acceso para cada una de las áreas del Invima. Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, teniendo en cuenta el tiempo de ejecución de contrato para estos últimos. Implementar las directrices de seguridad para el acceso a la información	Responsables de las áreas y procesos del Invima. Grupo de Soporte Tecnológico Oficial de seguridad de la información	01/02/2021	31/12/2021
Definición y socialización de las rutas digitales para el almacenamiento de la información	Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento. Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por la oficina de tecnología.	oficial de seguridad de la información, oficina de tecnologías de la información y grupo de soporte tecnológico.	01/01/2021	01/06/2021

Nuevos controles

Control	Plan de mejora / Acciones	Responsable	Fechas de implementación	
			Inicio	Fin
Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información.	Realizar pruebas de restauración periódicas junto con el responsable de la información tomando al azar áreas o procesos que hayan identificado activos de información importantes en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo. Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos personales sensibles.	Grupo soporte tecnológico en conjunto con el propietario de la información o quien éste designe	01/02/2021	31/12/2021
Identificar riesgos de seguridad de la información en todos los proyectos y controles de cambios de la entidad	Tener en cuenta la visión de seguridad de la información la identificación de riesgos para la ejecución de nuevos proyectos dentro de la entidad, no solo para los proyectos de carácter tecnológico. Tener en cuenta el punto de vista de seguridad de la información en los controles de cambios para aplicativos desarrollados interna o externamente en la entidad.	Oficinas, áreas y procesos. Oficial de seguridad de la información	01/02/2021	30/08/2021
Documentar las acciones realizadas por mesa de ayuda	Sensibilizar a todos los miembros del equipo de soporte tecnológico frente a la importancia de la documentación que se debe tener en cualquiera de las acciones realizadas frente a configuraciones de permisos de acceso a la información, solicitud de borrado de información, entrega de información o actualizaciones a la información.	Grupo soporte tecnológico Oficial de seguridad de la información	01/02/2021	30/06/2021
Mejoras en los procesos y procedimientos qué administren información	Sensibilizar a todo el personal frente a la necesidad de incluir la protección de la información en los procesos o procedimientos que lo requieran. Definir metodologías o mecanismos de anonimización de la información ya sea ésta de forma digital (bases de datos, documentos electrónicos, entre otros) o impresa	Oficinas, áreas y procesos. Oficial de seguridad de la información	01/01/2021	31/12/2021

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 2021 se proponen los siguientes temas relacionados:

1- Adquisiciones que apoyen las copias de respaldo de la información del Invima ya sean éstas productos o servicios propios o contratados con terceros.
2- contratación de una ética al hacking qué comprueben vulnerabilidades internas y de la red en el Invima.
3- 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.

12. DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS DE INVERSIÓN

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

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

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

13. INDICADORES

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

14. MAPAS DE RIESGOS

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

15. REQUERIMIENTO DE PERSONAL

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

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