PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C., enero de 2024

TABLA DE CONTENIDO

1 ALCANCE DEL PLAN 3
2 OBJETIVO 3
2.1 OBJETIVOS ESPECÍFICOS 3
3 ESTRATEGIAS 3
4 CONTINUACIÓN CIERRE DE BRECHAS ENCONTRANDAS EN LA REVISIÓN TÉCNICA INDEPENDIENTE DEL 2020 4
5 CIERRE DE BRECHAS DE AUDITORÍA REALIZADA 4
6 REVISIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 4
7 REVISIÓN POR LA DIRECCIÓN DEL AVANCE DEL PLAN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 5
8 METAS 5
9 ACCIONES 5
10 PRODUCTOS 8
11 RESPONSABLES 8
12 CRONOGRAMA 8
13 PLANES GENERALES DE COMPRAS QUE DESAGREGUEN LOS RECURSOS ASOCIADOS A TODAS LAS FUENTES DE FINANCIACIÓN ..... ¡Error! Marcador no definido.
14 INDICADORES ..... ¡Error! Marcador no definido.
15 MAPAS DE RIESGOS ..... ¡Error! Marcador no definido.
16 REQUERIMIENTO DE PERSONAL ..... ¡Error! Marcador no definido.

1 ALCANCE DEL PLAN

La implementación, gestión y operación del Sistema de Gestión de Seguridad de la Información - SGSI, se realiza en todos los procesos del Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA, de acuerdo con el ciclo de mejora continua PHVA; esto incluye, las actividades de formalización de los procesos, procedimientos y documentación correspondiente al SGSI a través de su integración con el Sistema de Gestión Integrado – SGI donde se manifiesta lo siguiente:

“El Invima diseña, promueve y adoptas las medidas necesarias que permitan disponer, gestionar y proteger la información suministrada a la entidad y generada por la misma de las diferentes amenazas que pueden afectar la integridad, disponibilidad y confidencialidad de la información. Identificando y gestionando los riesgos de forma eficiente y efectiva en todos los procesos, incorporando como resultado de esta gestión la mejora continua en materia de seguridad de la información, entendiendo que esta puede encontrarse en medios electrónicos y físicos.”

2 OBJETIVO

Este plan tiene como objetivo determinar las acciones que se realizaran para proteger la información que el Instituto Nacional de Vigilancia de Medicamentos y Alimentos INVIMA utiliza para proteger y promover la salud de la población, mediante la gestión del riesgo asociada al consumo y uso de alimentos, medicamentos, dispositivos médicos y otros productos objeto de vigilancia sanitaria.

2.1 OBJETIVOS ESPECÍFICOS

- Revisar, actualizar las políticas y documentos existentes
- Divulgar e implementar el SGSI
- Hacer seguimiento al cierre de brechas resultado de la auditoría interna
- Definir indicadores
- Evaluar el SGSI
- Certificar el SGSI

3 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:

- Sensibilizar a las diferentes áreas y procesos de la entidad sobre las responsabilidades que tienen frente a la protección y acceso a la información.
- 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.
- Implementar acciones que permitan cerrar las brechas encontradas en la auditoría interna realizada en el 2020.
- Capacitar a los servidores públicos en la identificación y tratamiento de los riesgos de seguridad de la información y la identificación de los activos de información, así como su valoración.

4 CONTINUACIÓN CIERRE DE BRECHAS PARA LA MITIGACIÓN DE VULNERABILIDADES

Continuar junto con la Oficina de Tecnologías de la Información con el seguimiento al plan de acción para la mitigación de todas las vulnerabilidades encontradas en el ejercicio del hacking ético del 2020.

5 CIERRE DE BRECHAS BASADOS EN PORCESOS DE AUDITORÍAS

De acuerdo con los resultados de la auditorías internas realizadas en años anteriores, basados en el cumplimiento de la norma ISO 27001:2013, y en las acciones de seguimiento y control basados en la definición de los riegos identificados en materia de seguridad de la información, se deben adelantar de forma conjunta con la Oficina de Tecnologías de la Información y las demás áreas del Invima, los planes de acción para avanzar en el cierre de brechas de vulnerabilidades o debilidades en el marco de la seguridad informática y de la información.

6 FORMACIÓN EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Se propenderá por buscar el acceso a formación en materia de seguridad de la información, con el fin de empoderar al personal con las habilidades necesarias para identificar, prevenir y responder a posibles amenazas cibernéticas. Esto incluye la formación en buenas prácticas de seguridad, concientización sobre amenazas actuales, y la promoción de una cultura proactiva en la prevención de incidentes de seguridad. Un equipo bien capacitado se convierte en una primera línea de defensa fundamental contra las amenazas en constante

evolución en el entorno digital del INVIMA

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

Se plantean 4 revisiones por la dirección en el año 2024, donde se deberá:

- Socializar el avance de implementación del presente plan.
- Dar a conocer el seguimiento al plan de tratamiento de riesgos de seguridad de la información.
- Identificar los requerimientos de apoyo o intervención por parte de la dirección.
- Seguimiento a indicadores del SGSI.

8 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.

9 ACCIONES

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

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

Gestión	Actividades	Tareas	Responsable de la Tarea
		Información, Cambios físicos de la ubicación de activos 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.	Oficial de Seguridad de la Información
		Publicar los instrumentos de activos de información consolidado en transparencia	Oficial de Seguridad de la 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 privacidad de la Información en INTEGRA	Oficial de seguridad de la información
	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
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información
	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	Oficina Asesora de 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
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Responsable de cada área o proceso, facilitador, 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
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Oficina Asesora de Planeación
Gestión de Incidentes de		Revisión, actualización y publicación del procedimiento de incidentes de	Oficial de Seguridad de la Información

Gestión	Actividades	Tareas	Responsable de la Tarea
Seguridad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	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	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 con 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 - OTI
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información
		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los facilitadores de procesos	Oficial de Seguridad de la Información
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información – Grupo de Comunicaciones
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información – Grupo de Comunicaciones
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 - Oficina Asesora Jurídica
	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 - Oficina Asesora Jurídica
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 – OTI - Oficina Asesora 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 – OTI - Oficina Asesora 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 – OTI - Oficina Asesora Jurídica

10 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 ISO27001:2013 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, documentado e incluido en el mapa de procesos de la Entidad
- Inventario de Activos de Información actualizado
- Riesgos de seguridad de la Información identificados y gestionados
- Gestión de incidentes de Seguridad de la Información atendidos
- Plan de gestión del cambio y cultura de Seguridad y Privacidad de la Información
- Matriz de verificación de requisitos legales de Seguridad de la Información
- Inventario de Protección de datos personales actualizado

11 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.

Además de las responsabilidades específicas ya definidas de acuerdo con lo estipulado en el anexo de la norma ISO 27001:2013.

12 CRONOGRAMA

De acuerdo con las actividades definidas se presenta el cronograma con vigencia al 2024

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 2024	18 de Feb de 2024
	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 2024	15 de marzo de 2024
		Validar activos de información en el	Responsable de cada área o	15 de marzo de 2024	30 de junio 2024

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		instrumento levantado en la vigencia anterior	proceso y facilitador		
		Identificar nuevos activos de información en cada dependencia	Responsable de cada área o proceso y facilitador	15 de marzo de 2024	30 de junio 2024
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Equipo de información	15 de marzo de 2024	30 de junio 2024
		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 2024	30 de junio 2024
		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	01 de julio de 2024	30 de agosto de 2024
	Publicación de Activos de Información y registros activos de información ley 1712	Validar y aceptar los activos de información para su publicación en transparencia por cada líder de proceso.	Responsable de cada área o proceso y facilitador	01 de sept de 2024	15 de sept de 2024

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		Consolidar el instrumento de activos de Información.	Equipo de información	15 de sept de 2024	30 de sept de 2024
		Publicar los instrumentos de activos de información consolidado en transparencia	Equipo de información	1 oct de 2024	15 de dic de 2024
	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 2024	15 de dic de 2024
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 2024	30 de marzo de 2024
	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 2024	30 de marzo de 2024
		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 2024	30 de marzo de 2024
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Responsable de cada área o proceso y facilitador	01 de Feb de 2024	30 de marzo de 2024

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	Publicación	Publicación Matriz de riesgos	Planeación	01 de Feb de 2024	30 de marzo de 2024
	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 2024	30 de agosto de 2024
	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 2024	30 de agosto de 2024
	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 2024	30 de nov de 2024
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Planeación	30 de nov de 2024	15 de dic de 2024
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 2024	30 de dic de 2024
		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 2024	30 de dic de 2024

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		Socializar el procedimiento a los colabores de la Entidad.	Oficial de Seguridad de la Información	24 de enero de 2024	30 de dic de 2024
	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	24 de enero de 2024	30 de dic de 2024
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información	24 de enero de 2024	30 de dic de 2024
	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 2024	30 de dic de 2024
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información	24 de enero de 2024	15 de feb de 2024
		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los facilitadores de procesos	Oficial de Seguridad de la Información	15 de Feb de 2024	01 de marzo de 2024
	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 2024	30 de dic de 2024
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información - Comunicaciones	01 de marzo de 2024	30 de dic de 2024

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficial de Seguridad de la Información - Jurídica	01 de agosto de 2024	30 de sept de 2024
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficial de Seguridad de la Información - Jurídica	01 de agosto de 2024	30 de sept de 2024
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 febrero de 2024	15 de marzo de 2024
	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 2024	01 jun de 2024
	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 2024	30 de jul de 2024

13 PLANES GENERALES DE COMPRAS

Dentro de los planes presupuestados por la Oficina de Tecnologías de la Información del Invima, se han establecido proyectos para ayudar con la mitigación de los riesgos de seguridad de la información en el periodo del 2024 al 2027, en este sentido se atiende el proyecto asociado a ciberseguridad del PETI 2024 - 2027:

- Plan proyecto fortalecimiento de la seguridad informática del Invima, basa en el PETI del Invima 2024 – 2027

14 DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS DE INVERSIÓN

La distribución presupuestal proyectada a mediano plazo en el PETI 2024 – 2027 de los proyectos de inversión enfocados en materia de Ciberseguridad es:

Línea Estratégica	Producto POAI	Proyecto	Linea Acción	Actividad	Presupuesto 2024	2025	2026	2027	TOTAL
Innovación Tecnológica	Servicios Tecnológicos - Servicios de información para la gestión de la inspección, vigilancia y control sanitario	Implementación de la Fábrica de Software	Mejoramiento y Soporte a los Sistemas de Información.	Nueva Plataforma	$ 3.338.667.372	$ 3.599.083.427	$ 3.879.811.935	$ 4.182.437.266	$ 15.000.000.000
				Sivicos III					
				Silab					
				Portal Web					
				Intranet Inst.					
				Gestor Documental					
				Inventarios					
				Planeación					
				Gestor de cuentas					
				Contractual					
				Nomina					
			Desarrollo de Nuevos Sistemas de Información de apoyo	Intranet Inst.					
				Gestor Documental					
				Inventarios					
				Planeación					
				Gestor de cuentas					
				Contractual					
				Nomina					
				Financiero					
			Desarrollo de Nuevos Sistemas de Información misionales						
	Servicios de información para la gestión de la inspección, vigilancia y control sanitario	Implementación de Inteligencia de Negocios Fase III		Analítica de Datos	$ 979.342.429	$ 1.055.731.139	$ 1.138.078.168	$ 1.226.848.265	$ 4.400.000.000
				Georeferenciación					
Modernización de la infraestructura tecnológica	Servicios Tecnológicos	Fortalecimiento de la infraestructura de TI	Adquisición de Hiperconvergencia		$ 13.799.825.139	$ 14.876.211.500	$ 16.036.555.997	$ 17.287.407.365	$ 62.000.000.000
			Adquisición Sistema de Backup						
			Adquisición Sistema Firewall y WAF y mejoras para ciberseguridad						
			Adquisición de Balanceador de Cargas						
			Implementación IPV6 - GTTS y PAPF						
			Contratación del SOC institucional						
Implementación de la Política de Gobierno Digital	Doumentos metodológicos	Implementación de la Política de Gobierno Digital	Adopción e implementación de la Arquitectura Empresarial en TI.	Implementación y mejora continua del Modelo de Arquitectura Empresarial MAE	$ 1.357.724.731	$ 1.463.627.260	$ 1.577.790.187	$ 1.700.857.821	$ 6.100.000.000
				Implementación y mejora continua del Modelo de Gestión de Proyectos MGPTI.					
				Implementación y mejora continua del Modelo de Gestión y Gobierno de TI MGGTI.					
			Fortalecimiento de la Cultura, Uso y Apropiación de TI en la Institucion.	Apropiación de ITIL en servicios tecnológicos					
				Desarrollo de capacidades para el uso y apropiación de TI					
				Apropiación de metodología de Gestión del Cambio.					
			Fortalecimiento de las metodologías y mejores prácticas de desarrollo de software.	Implementación de las metodologías.					
				Mejora Continua de las capacidades y mejores prácticas.					
			Fortalecimiento de la Seguridad Informática.	Implementación y seguimiento de políticas, lineamientos, guías, manuales y documentos Seguridad Informática.					
				Fortalecimiento de las capacidades y conocimientos en aspectos de seguridad informática.					
Operación de tecnología					$ 15.068.518.740	$ 16.243.863.202	$ 17.510.884.532	$ 18.876.733.525	$ 67.700.000.000
Total Presupuesto 2024 2027					$ 34.544.078.412	$ 37.238.516.528	$ 40.143.120.818	$ 43.274.284.241	$ 155.200.000.000

15 INDICADORES

El indicador definido para el proceso de Gestión de Seguridad de la Información:

Id	Nombre	Proceso	Sentido	Tipo	Clasificación	Ver
438	SGI- Nivel de madurez de los controles de seguridad de la información.	GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Hacia arriba	Eficacia	Operativo	Ver

INTEGRA Sistema de Gestión Integrado | invima

Id 438. SGI- Nivel de madurez de los controles de seguridad de la información.

Descripción	Proceso	Responsable
Establecer el nivel de madurez de los controles implementados en el Sistema de Gestión de Seguridad de la Información con el fin de generar un plan de Seguridad de la Información que sea desarrollado al interior de la entidad para dar cumplimiento a la política de gobierno digital y MIPG	GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (subproceso)	

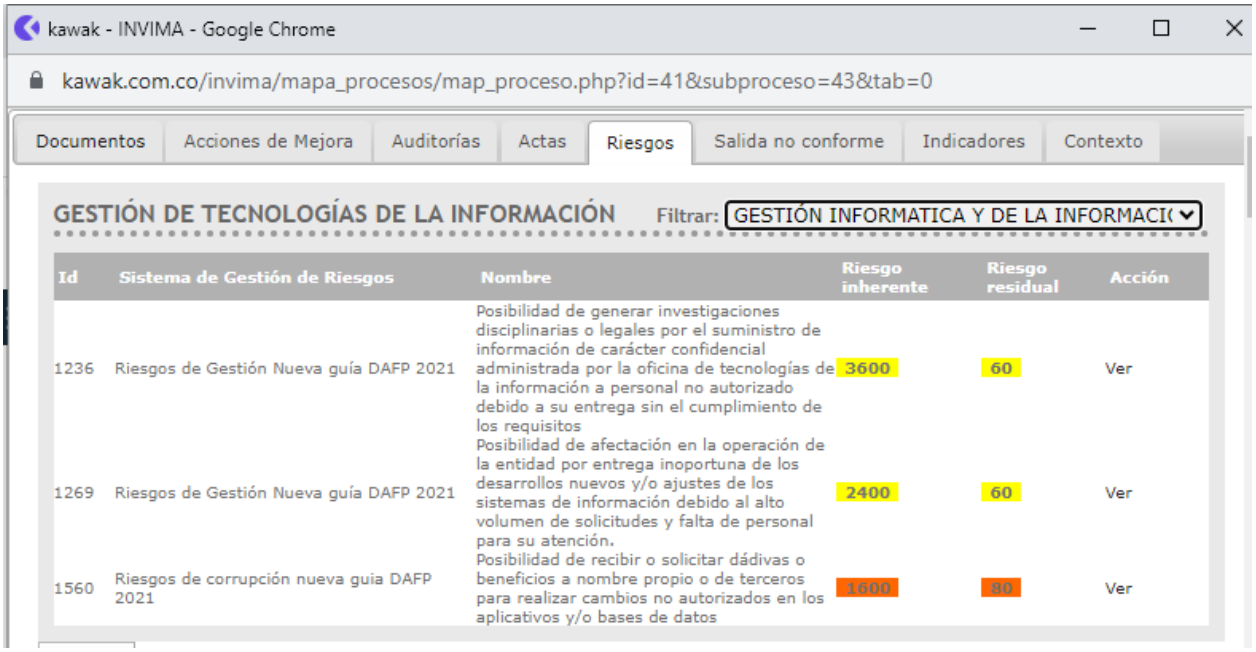
Fuente https://www.kawak.com.co/invima/ind_indicador/uvi_ver.php?llave=438

16 MAPA DE RIESGOS

Definición y gestión de la Matriz riesgos de TI a nivel general

La Oficina de Tecnologías de la Información (OTI), cuenta con matriz de riesgos de corrupción, matriz de riesgos para Gestión Informática y de la Información, así como, de Seguridad Informática. A continuación, se presenta de las fuentes Sistema de Gestión Integrado INTEGRA (Kawak) y de información recibida de la Oficina Asesora de Planeación:

Matriz de Riesgos de Corrupción:



Fuente: https://kawak.com.co/Invima/mapa_procesos/map_proceso.php?id=41&subproceso=43&tab=8

Matriz de Riesgos de Corrupción

ID	Fecha identificación	Nombre	Consecuencia	Probabilidad	Impacto	Zona inherente
5097	2020-12-02	Posibilidad de recibir o solicitar dádivas o beneficios a nombre propio o de terceros para realizar cambios no autorizados en los aplicativos y/o bases de datos	Sistemas de información vulnerados - Pérdida de información o información no confiable - Pérdida de imagen institucional - Imposición de	20	80	Alto

			sanciones legales, penales y económicas			
5110	2021-01-07	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para la interrupción de los servicios a través de acciones premeditadas en el centro de datos	Interrupción en la prestación de servicios - Retrasos en la operación de la entidad - Disminución o pérdida de productividad - Perdida, daños, manipulación, robos en la información y/o infraestructura tecnológica - Insatisfacción de los usuarios internos del Invima - Indisponibilidad de los servicios tecnológicos - Pérdida de imagen corporativa - Incremento de costos - Sanciones disciplinarias, fiscales, penales - Detrimento patrimonial - Incumplimiento de objetivos y metas institucionales	60	80	Alto
5119	2021-01-08	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para la creación de usuarios y la asignación de privilegios de acceso y roles no autorizados	Investigación a funcionarios implicados en casos de corrupción - Imagen de la entidad afectada - Pérdida de información - Acciones disciplinarias, penales, administrativas y fiscales	40	80	Alto

Matriz de Riesgos Gestión Informática y de la Información:

Fuente: https://kawak.com.co/Invima/mapa_procesos/map_proceso.php?id=41&subproceso=44&tab=8

Tabla. matriz de Riesgos Gestión Informática y de la Información

ID	Fecha identificación	Nombre	Consecuencias	Probabilidad	Impacto	Zona inherente
3044	2021-03-24	Posibilidad de afectación económica y perdida de información, por multas, sanciones de las entidades reguladoras o difusión de software dañino, debido al uso de software no autorizado en el Instituto.	- Demandas legales - Fraudes en línea - Multas, sanciones al Instituto debido al Uso de software no licenciado - Perdida de la credibilidad del área de tecnología. - Caídas del sistema por malware - Pérdida de datos o información - Daño en software y Hardware por instalación de aplicaciones no confiables	60	60	Moderado
3031	2021-03-24	Posibilidad de generar investigaciones disciplinarias o legales por el suministro de información de carácter	- Entrega de información a personas no autorizadas - Pérdida de imagen institucional - Apertura de proceso disciplinario - Demandas contra el Invima	60	60	Moderado

ID	Fecha identificación	Nombre	Consecuencias	Probabilidad	Impacto	Zona inherente
		confidencial administrada por la oficina de tecnologías de la información a personal no autorizado debido a su entrega sin el cumplimiento de los requisitos				
3048	2021-03-24	Posibilidad de afectación en la operación del instituto por la inoportuna expedición de documentos o actos administrativos debido a retrasos en la contratación de proveedores para firmas digitales para los funcionarios del Invima	- Inoportuna gestión de procesos dentro de aplicaciones institucionales y/o expedición de actos administrativos - Afectación a la imagen institucional - Inoportunos movimientos financieros	60	60	Moderado
3183	2019-08-30	Posibilidad de afectación de la operación de la entidad, por la indisponibilidad del activo de información, debido a las fallas de software y hardware del centro de datos	- Perdida de información - Demoras en los procesos y/o operación - Incremento de costos - Atención parcial o nula al ciudadano - Pérdida de imagen Institucional - Insatisfacción de los usuarios internos del Invima - Daños irreversibles en equipos tecnológicos y herramientas tecnológicas - Disminución o pérdida de productividad	80	100	Extremo
3031	2021-03-24	Posibilidad de afectación en la operación de la entidad por entrega inoportuna de los desarrollos nuevos y/o ajustes de los sistemas de información debido al alto volumen de solicitudes y falta	- Sanciones en contra de Invima - Insatisfacción de los funcionarios y usuarios - Demoras en los trámites del Invima - Detrimento de la Imagen institucional por las quejas y/o reclamos de los usuarios externos - Retrasos en el cumplimiento de los entregables en la operación misional	40	60	Moderado

ID	Fecha identificación	Nombre	Consecuencias	Probabilidad	Impacto	Zona inherente
		de personal para su atención.				
3031	2021-03-24	Posibilidad de afectación de la operación de la entidad por la pérdida de información debido a fallas internas o externas de las copias de respaldo.	- Pérdida de la integridad y disponibilidad de la información de misión crítica - Reprocesos - Afectación de la imagen Institucional - Investigaciones disciplinarias - Pérdida de recursos económicos.	60	60	Moderado
3222	2021-03-24	Posibilidad de pérdida o alteración de la información por la desactivación inoportuna, desactualización o creación indebida de usuarios.	- Fuga de Información - Modificación o consulta no autorizada de información - Afectación a la imagen institucional - Pérdida de información	60	60	Moderado

Matriz de Riesgos de Gestión de la Seguridad Informática

Fuente: https://kawak.com.co/Invima/mapa_procesos/map_proceso.php?id=41&subproceso=45&tab=8