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

Bogotá D.C., 2024

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.

2.1 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.

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

- 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.
- Generar alianzas entre procesos de apoyo que administren y gestionen controles que permitan proteger la información del Invima.
- Implementar acciones que permitan trabajar en equipos interdisciplinarios generando sinergias entre los diferentes procesos para proteger la información.

4 PLAN DE TRABAJO

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 las actividades definidas 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

5 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.

6 ACCIONES

De acuerdo con la guía 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
	Eventos/vulnerabilidades

7 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

Gestión	Actividades	Tareas
	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
		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 con 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

8 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

Gestión	Actividades	Tareas	Responsable de la Tarea
			seguridad de la información y Padrinos
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Responsable de cada área o proceso, facilitador, Oficial de seguridad de la información y Padrinos
	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 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 - Soporte Tecnológico - OTI

9 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 2024	30 de marzo de 2024
	Identificación de Riesgos de Seguridad y Privacidad	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la	Responsable de cada área o proceso, facilitador, Oficial	01 de Feb de 2024	30 de marzo de 2024

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	de la Información y Seguridad Digital	Información y Seguridad Digital	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	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
	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
		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

10 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 proponen los siguientes temas relacionados:

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

11 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 ecológica.	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

12 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 invima

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

Descripción	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	Proceso	GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (subproceso)	Responsable	

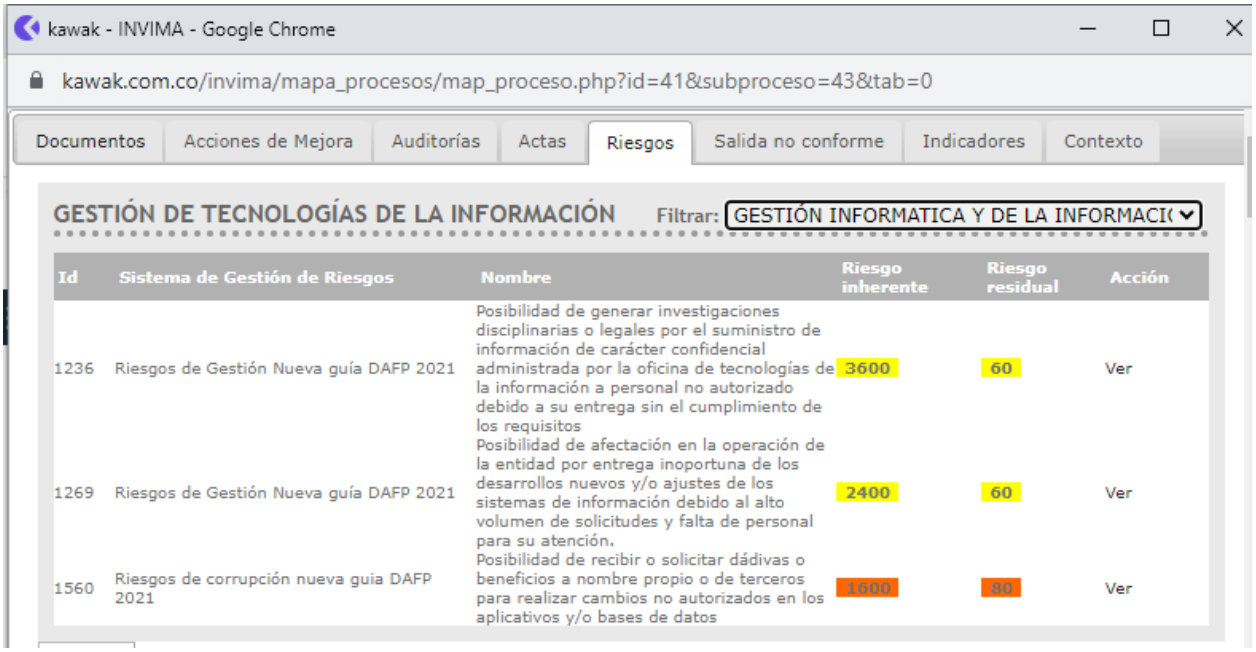
Fuente https://www.kawak.com.co/invima/ind_indicador/uvi_ver.php?llave=438

13 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

14. Fortalecimiento de la Seguridad Informática.

La Oficina de Tecnologías de la Información planea el desarrollo de un proyecto de "Fortalecimiento de la Seguridad Informática" en el INVIMA, el cual es fundamental para salvaguardar la integridad, confidencialidad y disponibilidad de la información crítica relacionada con su quehacer misional. Esta actividad se vuelve esencial en un contexto donde la seguridad de los datos y la protección contra amenazas cibernéticas son imperativos para cumplir con las regulaciones y mantener la confianza pública. El fortalecimiento de las medidas de seguridad informática no solo mitiga riesgos como el acceso no autorizado o la pérdida de datos, sino que también garantiza la continuidad de las operaciones y la resiliencia del INVIMA frente a las crecientes amenazas cibernéticas. Además, al promover una cultura organizacional consciente de la seguridad, este proyecto contribuye a la creación de un entorno seguro y confiable para la gestión eficiente de los procesos y datos críticos de la institución.

En este sentido se establecen dos actividades principales, estas actividades garantizan no solo la implementación efectiva de medidas de seguridad, sino también la construcción de una cultura organizacional consciente y preparada para enfrentar los desafíos de seguridad informática. Esto fortalece significativamente la posición del INVIMA frente a amenazas cibernéticas, asegurando la protección adecuada de la información vital en su misión reguladora de medicamentos y alimentos.

Implementación y seguimiento de políticas, lineamientos, guías, manuales y documentos Seguridad Informática.

Con esta acción se establece un marco de trabajo claro y normado en el INVIMA para el manejo de la información sensible. Esto no solo asegura la consistencia en las prácticas de seguridad, sino que también proporciona directrices claras para abordar amenazas potenciales y mantener la conformidad con regulaciones y estándares del sector. Asimismo, el seguimiento continuo garantiza la actualización y adaptación de estas políticas a medida que evolucionan las amenazas y las tecnologías.

Fortalecimiento de las capacidades y conocimientos en seguridad informática.

Con esta acción adicional, se espera 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.