Plan de Seguridad y Privacidad de la Información

Oficina de Informática y Desarrollo Tecnológico

Bogotá

2023-04-04

Instituto Nacional de Metrología de Colombia - INM
Av. Cra 50 No 26-55 Int. 2 CAN - Bogotá, D.C. Colombia
Conmutador: (57 601) 254 22 22 - **Website**: www.inm.gov.co
E-mail: contacto@inm.gov.co - **Twitter**: @inmcolombia
Código Postal 111321.

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO

CONTENIDO

Página.

1. INTRODUCCIÓN

Optimizar el plan de seguridad y privacidad de la información del INM con el fin de alinearse con la estrategia de gobierno en línea de Ministerio TIC, y la norma de seguridad ISO27001:2022 de tal forma que se establezcan los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de la información del INM.

2. ALCANCE

La implementación del plan se llevará acabo basado en los controles de la ISO27001:2022, los lineamientos de seguridad de gobierno en línea y el resultado del análisis de riesgos de seguridad de la información.

Se iniciará con una evaluación del estado actual del INM frente a los controles de seguridad de dicha norma y basados en este diagnóstico posteriormente se establecerá la optimización de los controles existentes y la implementación de los que no existan.

En el 2023 se hará una implementación inicial de los controles faltantes, para en el 2024, ir madurando el SGSI.

Los controles que requieran inversión se evaluará su viabilidad y si se salen del presupuesto se dejarán para implementar en 2024.

3. DESCRIPCIÓN METODOLÓGICA

El presente documento se estructura de conformidad a la metodología establecida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, capítulo 5 Lineamientos riesgos de seguridad de la información, 5.1. Identificación de los activos de seguridad de la información, 5.2. Identificación del riesgo, 5.3. Valoración del riesgo, 5.4 Controles asociados a la seguridad de la información del Departamento Administrativo de la Función Pública, versión 5, diciembre 2020.

3.1. MARCO NORMATIVO

NTC/ISO 27001:2022

Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL _ Habilitador Gobierno Digital -Seguridad – Decreto 1078 de 2015; Decreto 1008 de 2018.

3.2. DEFINICIONES

Activos: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000.

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

3.3. POLITICAS O LINEAMIENTOS GENERALES

- El plan será liderado por el responsable de seguridad de la información. Sin embargo, para el éxito de la implementación de éste es necesaria la participación de personal de diferentes áreas.
- Es necesario el compromiso y apoyo de la alta dirección.
- Para la implementación de los controles tecnológicos es necesario el compromiso y colaboración del personal de OIDT.
- Es necesaria la participación de otras áreas como Recursos humanos y Jurídico para optimizar los controles de personal.
- Todos los empleados y contratistas deben participar en actividades específicas que el plan lo requiera.

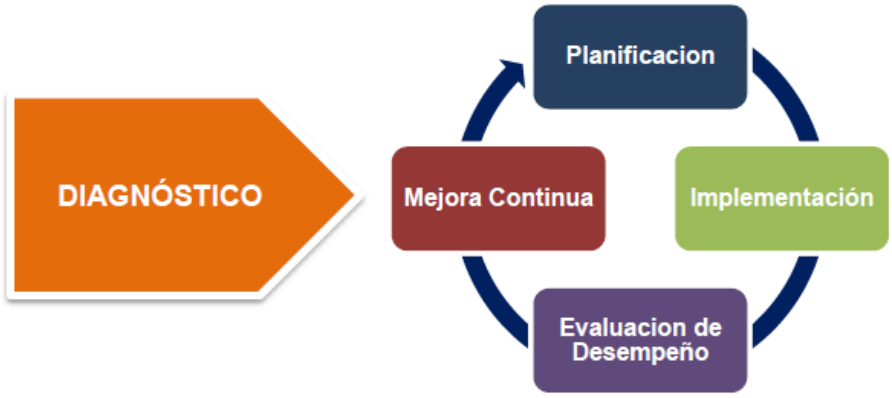
3.4. CONDICIONES DE SEGURIDAD

Todas las implementaciones resultantes del plan van orientadas a mantener la confidencialidad, disponibilidad e integridad de la información del INM.

3.5. DESCRIPCIÓN DE ACTIVIDADES O CONTENIDO PRINCIPAL

La seguridad y privacidad de la información, es un componente transversal a la Estrategia de Gobierno en línea. Este va alineado con la implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

El INM ha venido avanzando en la implantación de este modelo de seguridad y el objetivo es seguir madurándolo a través de este año 2023, cumpliendo con el ciclo de operación del modelo de seguridad y privacidad de la información, donde siempre se hace énfasis en una mejora continua.



Ciclo de operación del modelo de seguridad y privacidad de la información[1]

Para el desarrollo del plan se llevarán a cabo las fases planteadas en el modelo de seguridad y privacidad de la información:

- **Fase de diagnóstico**

Se realizará una revisión del estado de la seguridad del INM a través de herramienta de diagnóstico y levantamiento de información a través de entrevistas y revisión de documentación existente.

- **Fase de planificación**

[1] Modelo de seguridad y privacidad de la información. MinTIC

En esta fase, basado en la información recopilada en la etapa anterior, se elaborará el plan de seguridad y privacidad de la información el cual define las actividades a desarrollar a través del año para aumentar el nivel de seguridad actual del INM.

- **Fase de implementación**

En esta fase se da el cumplimiento al plan planteado en la fase de planificación. Esto implica revisión de matriz de riesgos de seguridad de la información, actualización de políticas de seguridad, procedimientos de tecnología, recursos humanos y seguridad física y definición de indicadores.

- **Fase de evaluación del desempeño y mejora continua**

Con base en la medición de los indicadores se establecen acciones de mejora y se evalúa el progreso del sistema de seguridad de la información.

3.5.1. Estándares utilizados para el desarrollo del Plan

Debido a la actualización de la norma ISO27001, a la versión 2022, la evaluación de diagnóstico se llevará basándose en dicha norma y se actualizará también el formato MSPI.

Los controles de la norma ISO27001:2022 a evaluar e implementar son los siguientes:

Controles de seguridad de la información ISO2001:2022		
No.	**Descripción del control**	**Relación con controles del Anexo A ISO27001:2013**
A5	**Controles organizacionales**	
A.5.1	Política de seguridad de la información	05.1.1, 05.1.2
A.5.2	Roles y responsabilidades de seguridad de la información	06.1.1
A.5.3	segregación de tareas	06.1.2

A.5.4	Responsabilidades de la dirección	07.2.1
A.5.5	Contacto con autoridades	06.1.3
A.5.6	Contacto con grupos especiales de interés	06.1.4
A.5.7	Inteligencia de amenzas	New
A.5.8	Seguridad de la información en la administración de proyectos	06.1.5, 14.1.1
A.5.9	Inventario de información y otros activos asociados	08.1.1, 08.1.2
A.5.10	Uso aceptable de la información y otros activos asociados	08.1.3, 08.2.3
A.5.11	Devolución de activos	08.1.4
A.5.12	Clasificación de información	08.2.1
A.5.13	Etiquetado de la información	08.2.2
A.5.14	Transferencia de información	13.2.1, 13.2.2, 13.2.3
A.5.15	Control de acceso	09.1.1, 09.1.2
A.5.16	Gestión de identidades	09.2.1
A.5.17	Authentication information	09.2.4, 09.3.1, 09.4.3
A.5.18	Derechos de acceso	09.2.2, 09.2.5, 09.2.6
A.5.19	Seguridad de la información en relación con proveedores	15.1.1
A.5.20	Abordar la seguridad de la información en los acuerdos con los proveedores	15.1.2
A.5.21	Gestionar la seguridad de la información en la información y la cadena de suministro de tecnologías de la comunicación (TIC)	15.1.3
A.5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	15.2.1, 15.2.2
A.5.23	Seguridad de la información en el uso de servicios cloud	New
A.5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	16.1.1

A.5.25	Evaluación y decisión sobre eventos de seguridad de la información	16.1.4
A.5.26	Respuesta a incidentes de seguridad de la información	16.1.5
A.5.27	Aprender de los incidentes de seguridad de la información	16.1.6
A.5.28	Recolección de evidencia	16.1.7
A.5.29	Seguridad de la información durante la disrupción	17.1.1, 17.1.2, 17.1.3
A.5.30	Preparación de las TIC para la continuidad del negocio	New
A.5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	18.1.1, 18.1.5
A.5.32	Derechos de propiedad intelectual	18.1.2
A.5.33	Protección de registros	18.1.3
A.5.34	Privacidad y protección de la información de identificación personal (PII)	18.1.4
A.5.35	Revisión independiente de la seguridad de la información	18.2.1
A.5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	18.2.2, 18.2.3
A.5.37	Procedimientos operativos documentados	12.1.1
A6	**Controles de personal**	
A.6.1	Proceso de selección	07.1.1
A.6.2	Términos y condiciones de empleo	07.1.2
A.6.3	Concientización, educación y capacitación en seguridad de la información	07.2.2
A.6.4	Proceso Disciplinario	07.2.3
A.6.5	Responsabilidades después de la terminación o cambio de empleo	07.3.1
A.6.6	Acuerdos de confidencialidad o no divulgación	13.2.4
A.6.7	Trabajo remoto	06.2.2
A.6.8	Informes de eventos de seguridad de la información	16.1.2, 16.1.3

A7	**Controles físicos**	
A.7.1	Seguridad de perímetro físico	11.1.1
A.7.2	Entrada física	11.1.2, 11.1.6
A.7.3	Asegurar oficinas, salas e instalaciones	11.1.3
A.7.4	Monitoreo de seguridad física	New
A.7.5	Protección contra amenazas físicas y ambientales.	11.1.4
A.7.6	Trabajar en áreas seguras	11.1.5
A.7.7	Escritorio y pantalla limpia	11.2.9
A.7.8	Emplazamiento y protección de equipos	11.2.1
A.7.9	Seguridad de los activos fuera de las instalaciones	11.2.6
A.7.10	Medios de almacenamiento	08.3.1, 08.3.2, 08.3.3, 11.2.5
A.7.11	Utilidades de apoyo	11.2.2
A.7.12	seguridad en el cableado	11.2.3
A.7.13	Mantenimiento de equipos	11.2.4
A.7.14	Eliminación segura o reutilización de equipos	11.2.7
A8	**Controles tecnológicos**	
A.8.1	Uso de dispositivos móviles	06.2.1, 11.2.8
A.8.2	Derechos de acceso privilegiado	09.2.3
A.8.3	Restricción de acceso a la información	09.4.1
A.8.4	Acceso al código fuente	09.4.5
A.8.5	Autenticación segura	09.4.2
A.8.6	Gestión de capacidad	12.1.3
A.8.7	Protección contra malware	12.2.1

A.8.8	Gestión de vulnerabilidades técnicas	12.6.1, 18.2.3
A.8.9	Gestión de la configuración	New
A.8.10	Eliminación de información	New
A.8.11	Enmascaramiento de datos	New
A.8.12	Prevención de fuga de datos	New
A.8.13	Copia de seguridad de la información	12.3.1
A.8.14	Redundancia de las instalaciones de procesamiento de información	17.2.1
A.8.15	Inicio sesión	12.4.1, 12.4.2, 12.4.3
A.8.16	Actividades de monitoreo	New
A.8.17	Sincronización de reloj	12.4.4
A.8.18	Uso de programas de utilidad privilegiados	09.4.4
A.8.19	Instalación de software en sistemas operativos	12.5.1, 12.6.2
A.8.20	Seguridad en redes	13.1.1
A.8.21	Seguridad de los servicios de red.	13.1.2
A.8.22	Separación de redes	13.1.3
A.8.23	Filtrado web	New
A.8.24	Uso de criptografía	10.1.1, 10.1.2
A.8.25	Ciclo de vida de desarrollo seguro	14.2.1
A.8.26	Requisitos de seguridad de la aplicación	14.1.2, 14.1.3
A.8.27	Principios de arquitectura e ingeniería de sistemas seguros	14.2.5
A.8.28	Codificación segura	New

A.8.29	Pruebas de seguridad en desarrollo y aceptación.	14.2.8, 14.2.9
A.8.30	Desarrollo subcontratado	14.2.7
A.8.31	Separación de los entornos de desarrollo, prueba y producción	12.1.4, 14.2.6
A.8.32	Gestión del cambio	12.1.2, 14.2.2, 14.2.3, 14.2.4
A.8.33	Información de prueba	14.3.1
A.8.34	Protección de los sistemas de información durante las pruebas de auditoría	12.7.1

El plan de seguridad y privacidad de la información de 2023 se encuentra en el Anexo SEGUIMIENTO AL PLAN de Seguridad y Privacidad de la Información - VIGENCIA 2023 de la OIDT.

El detalle de las actividades se presenta en el cronograma establecido en el siguiente capítulo, donde se muestra el porcentaje de avance esperado.

3.6. CRONOGRAMA 2023

No. ÍTEM	ACTIVIDAD	PRODUCTO / ENTREGABLE	PROGRAMACIÓN												META ANUAL	RESPONSABLE
			M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12		
1	Fase diagnóstica: Revisión de información existente, establecer estado actual de implementación de SGSI y MSPI	Documento Evaluación SGSI ISO27001: 2022 y MSPI				1									1	Responsable de seguridad de la información
2	Fase de Planeación: Establecer plan y cronograma de seguridad y privacidad 2023	Documento			1										1	Responsable de seguridad de la información

3	Fase de implementación: Actualizar matriz de activos	Matriz de activos en isolucion					1								1	Responsable de seguridad de la información
4	Fase de implementación: Actualizar procedimientos de seguridad y manual de políticas seguridad, según resultado del diagnóstico.	Procedimientos de controles de seguridad y manual de políticas de seguridad de la información actualizados			1	2	4	3	4	3	3	2	1		23	OIDT
5	Evaluación y desempeño: Gestionar el cierre de hallazgos asociados a seguridad de la información (17 hallazgos abiertos en isolucion)	Hallazgos cerrados en isolucion				1	2	2	2	2	2	2	2	2	17	Responsable de seguridad de la información y OIDT
6	Revisar informes de análisis de vulnerabilidades y Contratar servicios para definir y ejecutar análisis de vulnerabilidad 2023 a sistemas críticos y realizar remediaciones	Documento con vulnerabilidades y documento de seguimiento a remediaciones										1			1	Responsable de seguridad de la información y OIDT
7	Hacer capacitaciones de concientización en seguridad de la información: boletines y charlas	Material de capacitación				1		1		1		1		1	5	Responsable de seguridad de la información
Revisó: Oficina Asesora de Planeación						**Aprobó: Comité Institucional de Gestión y Desempeño CIGD N° 5 del 2023-03-29 y 2023-04-04**										

4. ANEXOS

Cronograma Plan de Tratamiento de Riesgos de la Información.

LILIANA PINEDA APONTE

Contratista Seguridad de la Información

Fecha: 2023-04-04