indumil colombia

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Documento firmado digitalmente:

REVISÓ	APROBÓ
Cr. (RA) Sonia Dolly Gutiérrez Carrillo Gerente de Tecnologías de la Información Leyda Nelcy Aguirre Martínez Profesional Master GTI Sergio Alberto Villada Agudelo Director de Riesgos y Transformación	Cr (RA) Oscar Alberto Jaramillo Carrillo Cargo: Vicepresidente Corporativo Ronald Jamilton Moreno Samaniego Jefe Oficina de Planeación

Elaborado por:
Nombre: Luisa Fernanda Pulido Paez
Cargo: Profesional GTI

LIBERADO: 2023-09-25
REVISIÓN: 3
CODIGO: IM OC GTI PE 002

2023-2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan Estratégico de Seguridad y Privacidad de la Información es un instrumento que soporta el Sistema Integrado de Gestión de Seguridad de la Información, en él se establecen las actividades pertinentes para proteger la información que procesa la Industria Militar de Colombia, estas actividades están enmarcadas en el cumplimiento de los requisitos establecidos en la estrategia de seguridad digital, Artículo 5 de la Resolución 500 de 2021, "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*".

El plan inicia con el diligenciamiento del "**Instrumento de Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información**", teniendo en cuenta el contexto interno y externo de la entidad. Esta plantilla contiene las secciones o etapas mínimas recomendadas, que deben seguir las entidades que quieran estructurar un PESI adecuadamente.

En el presente documento se muestran los resultados obtenidos en el auto diagnóstico realizado, así como la descripción de cada una de las actividades a seguir para la integración y mejora del sistema de seguridad y privacidad de la información.

2.OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2023-2024

2.1 OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Establecer los roles y responsabilidades de seguridad y privacidad de la información de la Industria Militar.
- Establecer los propietarios de los activos de información de la Industria Militar
- Proveer las pautas requeridas y necesarias para la adecuada identificación, clasificación y valoración de los activos de información de la entidad.
- Actualizar e implementar los riesgos de seguridad y privacidad de la información conforme a la Norma ISO 31000 y la guía para la administración del riesgo y el diseño de controles en entidades públicas.
- Establecer y comunicar el manual de controles de seguridad y privacidad de la información.
- Priorizar los proyectos para la correcta implementación del SGSI.

3. ALCANCE

El Plan Estratégico de Seguridad y privacidad de la Información comparte el alcance definido dentro del sistema Seguridad de la Información ISO 27001 al servicio de Procesamiento Electrónico de Datos.

4.TÉRMINOS Y DEFINICIONES

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Gestión de Riesgo:** proceso de identificación y evaluación de riesgos y la toma de acciones efectivas para reducirlos a un nivel aceptable. Incluye la valoración de riesgos; análisis costo beneficio de las acciones y controles de mitigación, y la selección, implementación y valoración de controles de seguridad.

- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

- **Incidente de seguridad de la información:** Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

- **Información:** es todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

- **Ingeniería social:** consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

- **SGSI:** Sigla del Sistema de Gestión de la Seguridad de la Información. (ISMS en inglés, Information Security Management System).

- **MSPI:** Seguridad y Privacidad de la Información.

5.DOCUMENTOS DE REFERENCIA

Normativas:

- **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley 1266 de 2008:** Disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1273 de 2009:** Se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Ley 1341 de 2009:** Por medio del cual se definen los conceptos y principios relativos a la sociedad de la información y otros aspectos relacionados con las tecnologías de la información y las comunicaciones.

- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Decreto 2364 de 2012:** Lineamientos estratégicos del Plan Nacional de Desarrollo 2010 - 2014 “Prosperidad para todos” es la reglamentación del uso de la firma electrónica.

- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Decreto 1078 de 2015:** Esta Versión incorpora las modificaciones introducidas al decreto único reglamentario del sector de tecnologías de la información y las comunicaciones a partir de la fecha de expedición.

- **Decreto 612 de 2018:** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa

- **Ley 1955 de 2019:** Por el cual se expide el plan Nacional de Desarrollo 2018-2022 Pacto por Colombia, Pacto por la equidad.

- **Ley 1978 de 2019:** Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones. Se determina el marco general para la formulación de las políticas públicas que regirán el sector de las TIC.

- **Conpes 3975 de 2019:** Política Nacional para la Transformación Digital e Inteligencia Artificial.

- **Resolución 1519 de 2020:** Estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

- **Conpes 3995 de 2020:** Política Nacional de Confianza y Seguridad Digital.

- **Resolución 500 de 2021:** "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital". Manual de Gobierno Digital – MINTIC.

- **Directiva presidencial 003 de 2021:** Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

- **Decreto 338 de 2022:** Por el cual se adiciona el Titulo~1 ~a Ml\~1 2º~~ Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".

- **Decreto 767 de 2022:** "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"'.

- **Decreto 1263 de 2022:** "Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública".

- **Resolución 460 de 2022:** Por la Cual Se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.

- **Resolución 746 de 2022:** Por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución 500 de 2021.

- **Directiva presidencial 02 de 2022:** Reiteración de la Política Publica en Materia de Seguridad Digital.

6.ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Industria Militar por medio de la Gerencia de Tecnologías de la Información ha delegado la responsabilidad de mantener el sistema de gestión de Seguridad de la Información, esta gerencia ha velado por la confidencialidad, integridad y disponibilidad del procesamiento electrónico de datos. (verificar contra el original).

Para identificar el nivel de madurez del modelo de seguridad y privacidad de la información en la entidad, se toma como referencia el Instrumento de Evaluación del MSPI que es una herramienta creada por el Ministerio de Tecnologías y las Comunicaciones MINTIC.

A continuación, se muestra el resultado de la evaluación de madurez del Modelo de Seguridad y Privacidad de la Información – MSPI identificado en el documento de autodiagnóstico, por cada uno de los dominios definidos en dicho modelo

Tabla 1. Nivel Madurez del dominio de Seguridad

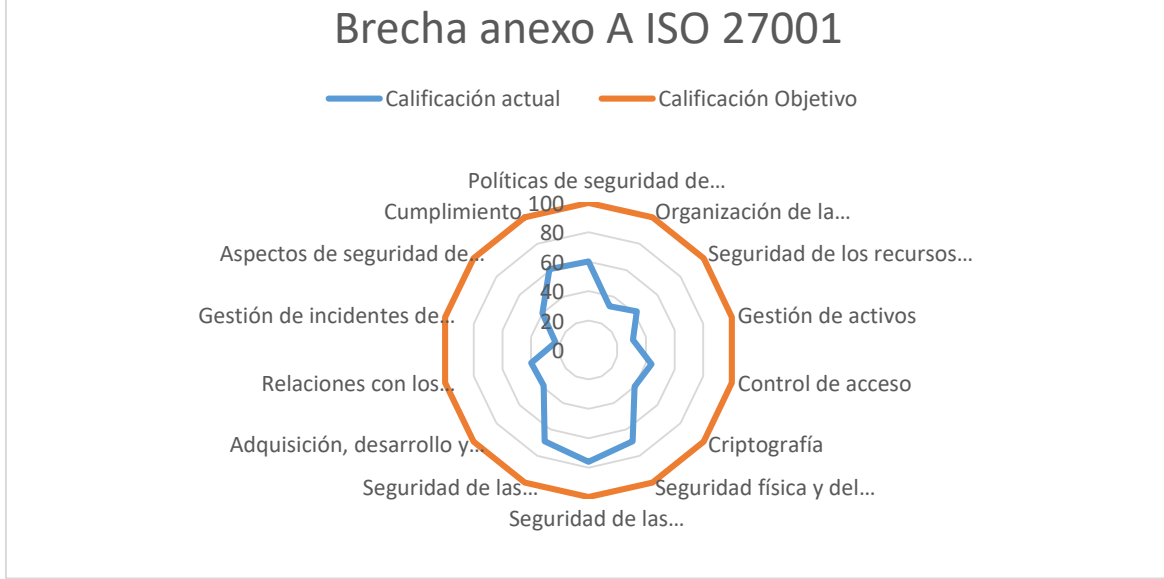
Id	Evaluación de efectividad de controles			
	Dominio	**Calificación actual**	**Calificación objetivo**	**Evaluación de efectividad de control**
A.5	Políticas de seguridad de la información	60	100	Efectivo
A.6	Organización de la seguridad de la información	33	100	Repetible
A.7	Seguridad de los recursos humanos	42	100	Efectivo
A.8	Gestión de activos	31	100	Repetible
A.9	Control de acceso	44	100	Efectivo
A.10	Criptografía	40	100	Repetible
A.11	Seguridad física y del entorno	69	100	Gestionado
A.12	Seguridad de las operaciones	76	100	Gestionado
A.13	Seguridad de las comunicaciones	69	100	Gestionado
A.14	Adquisición, desarrollo y mantenimiento de sistemas	39	100	Repetible
A.15	Relaciones con los proveedores	40	100	Repetible
A.16	Gestión de incidentes de seguridad de la información	23	100	Repetible
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	40	100	Repetible
A.18	Cumplimiento	61	100	Gestionado
Promedio evaluación de controles		**48**	**100**	Efectivo

Fuente: Instructivo para el diligenciamiento de la herramienta de diagnóstico de seguridad y privacidad de la información de MINTIC.

De la tabla anterior se puede concluir que actualmente la Industria Militar se encuentra en un nivel de madurez EFECTIVO con un valor promedio de 48 sobre un máximo de 100.

Por lo anterior se observa en la figura 1 el estado de los controles.

Figuras 1. Brecha anexa A ISO 27001



Fuente: Instructivo para el diligenciamiento de la herramienta de diagnóstico de seguridad y privacidad de la información de MINTIC.

El PHVA evalúa los componentes de planificación, implementación, evaluación de desempeño y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), teniendo como referencia el ítem de prueba conocidos como requisitos de cumplimiento.

Luego de realizar la calificación correspondiente, se observan los resultados comparando el avance actual de la entidad sobre el avance esperado, se obtiene:

Tabla 2. Avance ciclo de funcionamiento del modelo de operación

Año	AVANCE PHVA		
	Componente	**% de avance actual entidad**	**% avance esperado**
2023	Planificación	20%	40%
	Implementación	8%	20%
	Evaluación de desempeño	8%	20%
	Mejora continua	2%	20%
		38%	**100%**

Fuente: Instructivo para el diligenciamiento de la herramienta de diagnóstico de seguridad y privacidad de la información de MINTIC.

El estado de madurez en la herramienta del MSPI se miden bajo los niveles de madurez del modelo de seguridad y privacidad de la información que se describen a continuación:

Tabla 3. Niveles de madurez del MSPI

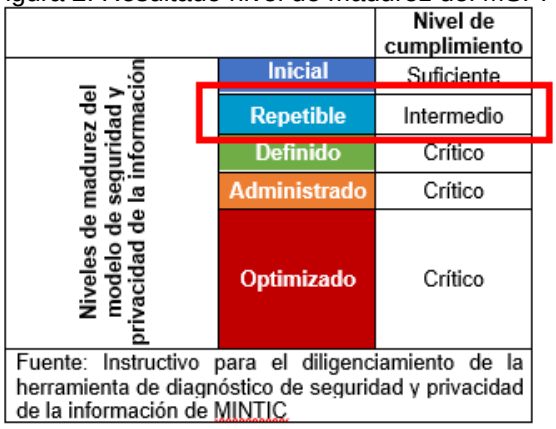
Nivel	Descripción
Inicial	En este nivel se encuentran las entidades que aún no cuentan con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto, los controles no están alineados con la perversión de la confidencialidad, integridad, disponibilidad y privacidad de la información.
Repetible	En este nivel se encuentra las entidades, en las cuales existen procesos básicos gestión de la seguridad y privacidad de la información, de igual forma existen controles que permite detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente de planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles
Optimizado	En este nivel se encuentran las entidades donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativa mente el modelo.
Fuente: Instructivo para el diligenciamiento de la herramienta de diagnóstico de seguridad y privacidad de la información de MINTIC	

Una vez realizada la calificación de los 55 requisitos, se obtuvo que la Industria Militar se encuentra en un nivel de cumplimiento intermedio (REPETIBLE) como se evidencia en la tabla de resultado nivel de madurez del MSPI.

Este nivel indica que existen procesos básicos de Gestión de Seguridad y Privacidad de la Información, existen controles los cuales ayudan a identificar posibles Incidentes de Seguridad, pero no se encuentra Gestionado dentro del MSPI.

La falla detectada es la falta de estandarización del modelo de Seguridad y Privacidad de la Información los controles no se encuentran en su totalidad documentados y/o actualizados, para permitir una correcta medición de los mismos y garantizar su efectividad.

Figura 2. Resultado nivel de madurez del MSPI

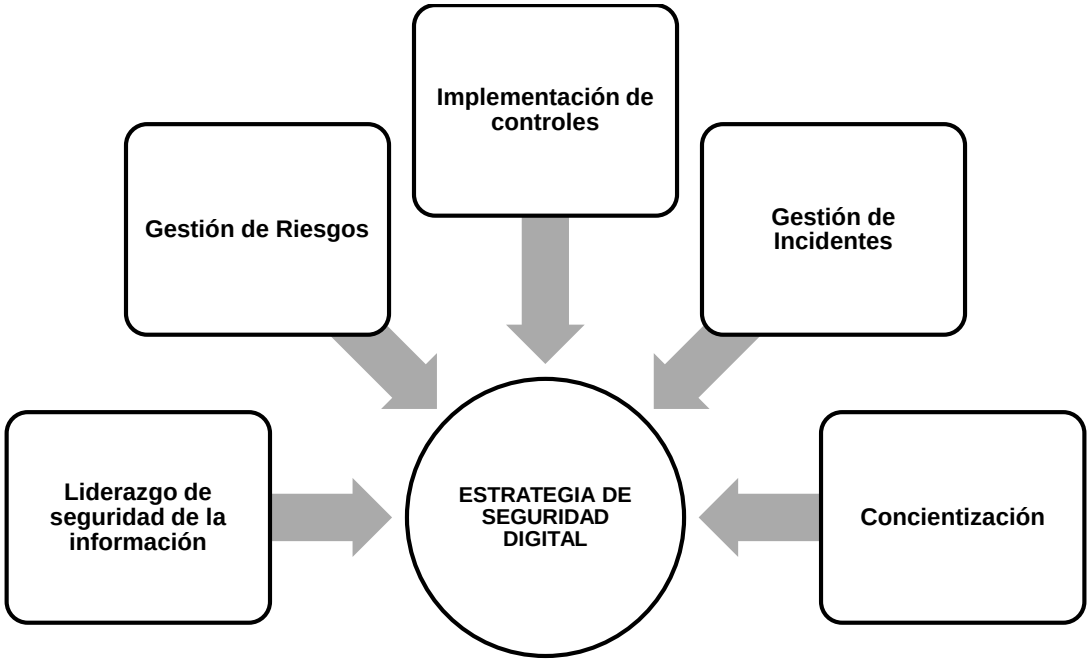


Fuente: Instructivo para el diligenciamiento de la herramienta de diagnóstico de seguridad y privacidad de la información de MINTIC

7. ESTRATEGIA DE SEGURIDAD DIGITAL

La Industria Militar establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes.

Por tal motivo, ***La Industria Militar*** define las siguientes 5 estrategias específicas,



7.1 Descripción de las estrategias específicas (ejes)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

8. PORTAFOLIO DE ACTIVIDADES

Para cada estrategia específica, **La Industria Militar** define los siguientes actividades y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ACTIVIDADES

ESTRATEGIA / EJE	ACTIVIDADES	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**ACTIVIDAD 1:** Reevaluar y actualizar la Política de seguridad y privacidad de la información conforme a las directrices del modelo del MSPI. **ACTIVIDAD 2:** Verificar y establecer los roles y responsabilidades de seguridad y privacidad de la información. **ACTIVIDAD 3:** Reevaluar el estado actual del sistema de seguridad de la información.	1. Política general de seguridad y privacidad de la Información formalizada. 2. Documento con roles y responsabilidades de seguridad de la Información formalizadas. 3. Autodiagnóstico del MSPI.
Gestión de riesgos	**ACTIVIDAD 1:** Reevaluar y actualizar los activos de información de la entidad conforme a las directrices del modelo del MSPI. **ACTIVIDAD 2:** Identificar, valorar y clasificar los riesgos asociados a los activos de información que se reevaluaron. **ACTIVIDAD 3:** Definir planes de tratamiento de riesgos de seguridad.	1. Matriz de Activos de Información por oficinas y Gerencias. 2. Matriz de riesgos de seguridad digital. 3. plan de tratamiento de riesgos de seguridad.

ESTRATEGIA / EJE	ACTIVIDADES	PRODUCTOS ESPERADOS
Concientización	**ACTIVIDAD 1:** Realizar Plan de sensibilización anual. **ACTIVIDAD 2:** Realizar jornadas de sensibilización a todo el personal de la entidad. **ACTIVIDAD 3:** Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializado en seguridad y privacidad de la información. **ACTIVIDAD 4:** Medir el grado de sensibilización a toda la Entidad.	1. Plan de sensibilización. 2. Evidencias de las actividades desarrolladas. 3. Certificaciones de cursos. 4. Resultado de las encuestas de medición.
Implementación de controles	**ACTIVIDAD 1:** Verificar y evaluar los controles actuales conforme a la identificación y reevaluación de nuevos riesgos. **ACTIVIDAD 2:** Establecer lista y/o manual de controles conforme a los lineamientos de Gobierno Digital.	1. Lista y/o manual de controles.
Gestión de incidentes	**ACTIVIDAD 1:** Reevaluar y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información conforme a los lineamientos de Gobierno Digital. **ACTIVIDAD 2:** Capacitar al personal en la gestión de incidentes de seguridad de la información. conforme a los lineamientos de Gobierno Digital	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas.

9. CRONOGRAMA DE ACTIVIDADES

AÑO 2023				AÑO 2024	
TRIMESTRE 1	**TRIMESTRE 2**	**TRIMESTRE 3**	**TRIMESTRE 4**	**TRIMESTRE 1**	**TRIMESTRE 2**
Autodiagnóstico del MSPI.	Política general de seguridad y privacidad de la Información formalizada	Matriz de Activos de Información por oficinas y Gerencias	Matriz de riesgos de seguridad digital	Matriz de Activos de Información por oficinas y Gerencias	Matriz de riesgos de seguridad digital
	Documento con roles y responsabilidades de seguridad de la Información formalizadas.		Plan de tratamiento de riesgos de seguridad.		Plan de tratamiento de riesgos de seguridad.
	Plan de sensibilización	Comunicación Tips de Seguridad de la Información.	Certificaciones de cursos	Certificaciones de cursos	Certificaciones de cursos
		Procedimiento de gestión de incidentes de seguridad formalizado	Lista y/o manual de controles.		
			Sesiones de capacitación desarrolladas.		

Nota: Al finalizar cada vigencia, La Industria Militar, realizará una actualización del cronograma, incorporando el estado del avance de las actividades formuladas y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

10. CRONOGRAMA DE PROYECTOS Y ANÁLISIS PRESUPUESTAL

Con base a los proyectos definidos, se genera el presupuesto aproximado por cada vigencia según los proyectos establecidos así:

AÑO 2023		AÑO 2024		AÑO 2025		AÑO 2026	
PROYECTO	**Inversión**	**PROYECTO**	**Inversión**	**PROYECTO**	**Inversión**	**PROYECTO**	**Inversión**
Licenciamiento de Antivirus	$ 156.800.000			Adquisición de nueva solución de ciberseguridad Endpoint	$200.000.000 (Proyectado)		
Solución de Seguridad perimetral y suscripción de licenciamiento	$ 845.971.000	Adquisición solución de seguridad Perimetral para OC	$330.000,000 (Proyectado)	Adquisición solución de seguridad Perimetral para las 3 fábricas de la IM	$500,000,000 (Proyectado)		
Servicio de mantenimiento y renovación Certificado Digital	$ 17.285.900						
		Adquisición e implementación WAF	$240,000,000 (Proyectado)				
				Sistema de ciberseguridad biométrica de dispositivos lógicos	$300.000.000 (Proyectado)	Sistema de seguridad Biométrica controles físicos	$300.000.000 (Proyectado)
TOTAL PRESUPUESTO AÑO 2023	**1.020.056.900**	**TOTAL PRESUPUESTO AÑO 2024**	**570.000.000**	**TOTAL PRESUPUESTO AÑO 2025**	**1.000.000.000**	**TOTAL PRESUPUESTO AÑO 2026**	$300.000.000

(Esta tabla solo muestra valores de referencia, cada entidad debe realizar los estudios de mercado correspondientes para tener plenamente identificados los costos aproximados de cada solución o proyecto, con base a la dimensión y necesidades específica.

11. CONTROL DE CAMBIOS

Motivo	Sección	Numeral	Página	Descripción de la modificación
Formato guia de MINTIC	Todo el documento	Todo el documento	Todo el documento	Se actualiza Nombre del Plan, adicionando la palabra estratégico. Se adiciona estratégica de Seguridad Digital. Se adiciona Cronograma de actividades. Se adiciona cronograma de proyectos y presupuesto proyectado.