Tabla de contenido

1. OBJETIVOS

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información y adelantar la gestión de estos riesgos en la Dirección General Marítima DIMAR.

2. ALCANCE

El presente documento responde a una necesidad fundamental, ya que la materialización de riesgos relacionados con la seguridad de la información puede comprometer el cumplimiento eficiente, efectivo y óptimo de los objetivos institucionales, tanto en el ámbito interno como en los servicios dirigidos a la ciudadanía. En este contexto, la gestión de riesgos de seguridad de la información se posiciona como una herramienta clave para el desarrollo, la implementación y la mejora continua de la Entidad, al garantizar la protección del valor organizacional mediante la seguridad de la información, tanto física como digital.
Con base en esta premisa, la Dimar formula el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2025, atendiendo a sus necesidades específicas en materia de seguridad de la información y asegurando el cumplimiento de las normativas aplicables. Este plan se alinea con los procesos de mejora continua, permitiendo gestionar de manera efectiva los hallazgos identificados durante la auditoría interna.

El Plan de Tratamiento de Riesgos tiene como objetivo definir las actividades a desarrollar durante el año 2025 para la identificación, análisis y control de los riesgos asociados a la Seguridad y Privacidad de la Información. Este plan se guía por el ciclo de Deming (PHVA: Planificar, Hacer, Verificar, Actuar) y se encuentra alineado con la Política de Seguridad de la Información de la Entidad, asegurando una gestión integral y efectiva de los riesgos que puedan afectar la seguridad y privacidad de la información.

3. GLOSARIO

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

Consecuencia: Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Vulnerabilidad: Debilidad, atributo, causa o falta de control que permitiría a explotación por parte de una o más amenazas contra los activos.

MSPI: Modelo de Seguridad y Privacidad de la Información.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO. Es certificable. Primera publicación en 2005, segunda publicación en 2013, tercera publicación en 2022.

4. DESARROLLO

A continuación, se describen las actividades a realizar, tiempo de ejecución y responsables:

4.1. Cronograma de ejecución del Plan

N°	NOMBRE DE LA TAREA	FECHA INICIAL	FECHA FINAL	RESPONSABLE
1	Actualización de la declaración de aplicabilidad de los controles ISO27001:2013.	01/02/2025	30/04/2025	Oficial de Seguridad de la Información
2	Actualizar matriz DOFA -factores externos e internos que puedan afectar la seguridad digital y de la información de acuerdo con los cambios en el contexto de la entidad.	01/03/2025	30/04/2025	Oficial de Seguridad de la Información
3	Gestionar el procedimiento para el tratamiento de riesgos de seguridad de la información del proceso E3. (P8 PHVA MATRIZ MSPI)	01/02/2025	30/06/2025	Oficial de Seguridad de la Información
4	Revisar la normatividad aplicable en: seguridad digital, datos personales, seguridad de la información, (Leyes, Decretos, Resoluciones, CONPES, etc.).	16/05/2025	18/09/2025	Oficial de Seguridad de la Información
5	Identificar, valorar y analizar los riesgos del Subsistema de Seguridad de la Información y de Seguridad informática del proceso E3. Incluye la revisión y actualización del mapa de riesgos (P6 PHVA MATRIZ MSPI)	3/02/2025	30/04/2025	Oficial de Seguridad de la Información
6	Efectuar medición trimestral del indicador Porcentaje de vulnerabilidades mitigadas para el análisis de vulnerabilidades.	03-02-2025 01-04-2025 01-07-2025 01-10-2025	04-04-2025 04-07-2025 03-10-2025 19-12-2025	Oficial de Seguridad de la Información
7	Realizar análisis de Impacto al Negocio (BIA) para sistemas de información críticos (Fase 2).	1/08/2025	30/10/2025	Oficial de Seguridad de la Información

N°	NOMBRE DE LA TAREA	FECHA INICIAL	FECHA FINAL	RESPONSABLE
8	Elaborar análisis y reporte de eventos de incidentes de seguridad de la información.	01/10/2025	30/11/2025	Oficial de Seguridad de la Información
9	Definición del DRP - Disaster Recovery plan - fase 2.	01/07/2025	30/09/2025	Oficial de Seguridad de la Información
10	Desarrollar Documento con el plan de seguimiento, evaluación y análisis para el MSPI, solicitar aprobación por la dirección (M1 PHVA MATRIZ MSPI)	1/02/2025	01/12/2025	Oficial de Seguridad de la Información

4.2. Seguimiento y Control del Plan

El control de las actividades del plan será efectuado por el Oficial de Seguridad de la Información de la Dimar, por medio de la presentación de informes de gestión, las actividades se encuentran cargadas como tareas y responsabilidades del Oficial de Seguridad de la Información en la plataforma SIMEC, con las cuales se realizará seguimiento a la ejecución de estas.

4.3. Indicadores del Plan

El plan será evaluado a través de un indicador estratégico que considera las variables de: **Planificación**, **Implementación**, **Evaluación de desempeño** y **Mejora continua** del MSPI, en este indicador se especificarán los avances de estas actividades.

Tabla 2. Indicador del plan

Indicador	Frecuencia	Responsable	Unidad Medida	Fórmula
Porcentaje de avance en la implementación de los controles ISO 27001 y del Modelo de Seguridad y Privacidad de la Información MSPI	Trimestral	Oficial de Seguridad la información	Porcentaje (%)	(Porcentaje avance fase de planificación del MSPI+Porcentaje Avance fase de Implementación+Porcentaje Avance fase de Evaluación del Desempeño+Porcentaje Avance fase de Mejora continua)*100