CONTENIDO

1. OBJETIVOS

1.1 Objetivo General

Adelantar la gestión de riesgos de seguridad de la información de la Dirección General Marítima DIMAR.

2. ALCANCE

El presente documento se convierte en una necesidad, toda vez que la materialización de los riesgos de seguridad de la información puede impedir el cumplimiento adecuado, efectivo y óptimo de los objetivos institucionales tanto internos como los dirigidos a la ciudadanía. Bajo esa perspectiva, la gestión de riesgos de seguridad de la información se presenta como una herramienta para el desarrollo, implementación y mejora continua de la Entidad partiendo de la protección del valor de la organización a partir de la seguridad de la información, tanto física como digital. La Dirección General Marítima establece el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia del 2024, de acuerdo con las necesidades de la Entidad frente a Seguridad de Información y al cumplimiento normativo correspondiente, dando continuidad a los procesos de mejora continua y dar gestión a los hallazgos encontrados en la auditoría interna.

El plan de tratamiento de riesgos busca establecer las actividades a realizar en el año 2024 para la identificación y análisis de los riesgos de Seguridad y Privacidad de la Información con sus correspondientes controles, orientado por el ciclo de Demming (PHVA) y alineado al cumplimiento de la Política de Seguridad de la Información de la Dirección General Marítima, en el entendido de gestionar los riesgos de seguridad y privacidad de la información de la Entidad.

3. GLOSARIO

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

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

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

Ataque cibernético: Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia)

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.

Confidencialidad: Propiedad de la información con la cual se garantiza que está accesible únicamente a personal autorizado para acceder a la misma.

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

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por la entidad.

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.

Integridad: Propiedad de exactitud y completitud.

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

Probabilidad: Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.

Tratamiento al riesgo: Respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

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

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 ISO27000	1/03/2024	31/05/2024	Líder Seguridad de la Información
2	Gestionar recurso de planta para el cargo OSI	1/04/2024	28/06/2024	Líder Seguridad de la Información
3	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.	3/06/2024	30/08/2024	Líder Seguridad de la Información

N°	NOMBRE DE LA TAREA	FECHA INICIAL	FECHA FINAL	RESPONSABLE
4	Revisar la normatividad aplicable en: seguridad digital, datos personales, seguridad de la información, (Leyes, Decretos, Resoluciones, CONPES, etc.).	3/06/2024	31/07/2024	Líder Seguridad de la Información
5	Actualización de la Guía, procedimiento y formato de gestión de incidentes	1/07/2024	30/09/2024	Líder Seguridad de la Información
6	Revisar y/o actualizar los riesgos de seguridad digital y de la información del proceso A3, incluye la revisión y actualización de la matriz de riesgos.	1/08/2024	31/10/2024	Líder Seguridad de la Información
7	Realizar análisis de Impacto al Negocio (BIA) para sistemas de información críticos (Fase I)	1/08/2024	31/10/2024	Líder Seguridad de la Información
8	Elaborar el plan operativo MSPI y de tratamiento de riesgos de seguridad informática frente a Ciberamenazas 2025	2/09/2024	29/11/2024	Líder Seguridad de la Información
9	Elaborar análisis y reporte de eventos de incidentes de seguridad de la información (Ciclo de vida)	2/09/2024	29/11/2024	Líder Seguridad de la Información
10	Identificación y Reporte de cumplimiento de los indicadores de seguridad para el análisis de vulnerabilidades	2/09/2024	29/11/2024	Líder Seguridad de la Información
11	Definir las responsabilidades para la gestión del riesgo de Seguridad de la Información y la aceptación de los riesgos residuales.	1/10/2024	10/12/2024	Líder Seguridad de la Información
12	Definición del DRP - Disaster Recovery plan - fase 1	1/10/2024	13/12/2024	Líder Seguridad de la Información

4.2. Seguimiento y Control del Plan

El control de las actividades del plan se efectuará mediante el seguimiento al contrato asignado para el líder de Seguridad de la Información, por medio de la presentación de informes de gestión y de supervisión mensuales, las actividades se encuentran cargadas como tareas y responsabilidades del Líder de Seguridad de la Información en la plataforma de SIMEC, con las cuales se realizará seguimiento a la ejecución de las mismas.

4.3. Indicadores del Plan

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

Tabla 2. Indicador del plan

Indicador	Frecuencia	Responsable	Unidad Medida	Fórmula
Avance en la implementación de los controles ISO 27001 y del Modelo de Seguridad y Privacidad de la Información MSPI	Trimestral	Líder de Seguridad la información	Porcentaje (%)	Avance Actual Entidad: % Planificación del MSPI + % Implementación MSPI + % Evaluación desempeño del MSPI + %Mejora continua MSPI