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 2023, 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 2023 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 PLANEADA	FECHA FINAL PLANEADA	RESPONSABLE
1	Revisar y/o actualizar los riesgos de seguridad de la información del proceso A3, incluyendo la definición de controles,	01-02-2023	31-08-2023	Líder Seguridad de la Información
2	Realizar el levantamiento de activos de información con los procesos priorizados de la Entidad – Fase II.	01-02-2022	15-12-2023	Líder Seguridad de la Información
3	Actualizar el plan de tratamiento de riesgos de seguridad informática frente a ciberamenazas.	30-07-2023	30-09-2023	Líder Seguridad de la Información

4	Revisar la aplicabilidad de nueva normatividad en materia de: seguridad digital, datos personales, seguridad de la información, (Leyes, Decretos, Resoluciones, CONPES, etc.).	10-02-2023	30-11-2023	Líder Seguridad de la Información
5	Implementar plan de capacitación de seguridad de la información de la vigencia.	01-01-2022	30-11-2023	Líder Seguridad de la Información

4.2. Seguimiento y Control del Plan

El control 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, y mediante plataforma SIMEC.

4.3. Indicadores del Plan

No dispone de indicador específico. Se realiza monitoreo de los riesgos de seguridad de la información a través de la plataforma SIMEC de manera trimestral.