Ministerio de Defensa Nacional
Dirección General Marítima
Autoridad Marítima Colombiana

PLAN

PLAN DE TRATAMIENTO DEL RIESGO

Proceso/Subproceso: Gobierno y gestión de las TIC

Código: A3-00-PLA-005

Versión: 0

1. INTRODUCCIÓN

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 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 la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia del 2022, 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.

2. OBJETIVOS

2.1. Objetivo General

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

2.2. Objetivos Específicos

a. Definir un cronograma de actividades que permita la administración y gestión de los riesgos de la entidad a nivel de Seguridad de la Información.

b. Establecer y ejecutar lineamientos y actividades puntuales para el tratamiento de riesgos de Seguridad y Privacidad de la Información en la DIMAR

3. ALCANCE

El plan de tratamiento de riesgos busca establecer las actividades a realizar en el año 2022 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)[1] y alineado al cumplimiento de la Política de Seguridad de la Información de la Dirección General Marítima, en el objetivo de gestionar los riesgos de seguridad y privacidad de la información de la Entidad.

4. CONCEPTOS TECNICOS

- **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).
- **Apetito de riesgo:** Máximo nivel de riesgo que los accionistas están dispuestos a aceptar. (Componente COSO ERM II)
- **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).
- **CCOC:** Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.
- **Causa:** Factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **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 que la hace no disponible, es decir divulgada a individuos, entidades o procesos no autorizados.
- **Control:** Medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

[1] Icontec. NTC-ISO-IEC 27001, Bogotá. 2013

- **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.
- **ICC**: Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su perturbación o destrucción tendría un grabe impacto sobre los servicios esenciales.
- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **Línea estratégica:** Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección, el equipo directivo, incluyendo el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno.
- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Política de administración del riesgo:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.
- **Primera línea de defensa:** Personas que se encuentras a cargo de gestionar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, está a cargo de los gerentes públicos y los líderes de procesos.
- **Probabilidad:** Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.
- **Riesgo de corrupción**: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgos de cumplimiento:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de imagen o reputacional:** Posibilidad de ocurrencia de un evento que afecten la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.
- **Riesgos de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.
- **Riesgos estratégicos:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización publica y por tanto impactan toda la entidad.
- **Riesgos financieros:** Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
- **Riesgos gerenciales:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
- **Riesgo inherente:** Riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgos operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
- **Riesgos tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- **Segunda línea de defensa:** Personas que asisten y guían a la línea estratégica y a la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)

- **Servicios Esenciales**: Servicios necesarios para el mantenimiento de las funciones sociales básicas la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del estado y las administraciones públicas.
- **Tercera línea de defensa:** Personas que provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera línea y la segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Está conformada por la Oficina de Control Interno o Auditoría Interna.
- **Tolerancia al riesgo:** Preparación de la organización o de la parte involucrada para soportar el riesgo después del tratamiento de este con el fin de lograr sus objetivos.
- **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.

5. MARCO NORMATIVO

La normatividad que rige a este documento puede encontrarse en el normograma establecido por la DIMAR

6. JUSTIFICACIÓN

El gobierno nacional plantea la política de Gobierno Digital, con la cual se genera un nuevo enfoque, en donde no sólo la Administración Pública sino también los diferentes actores de la sociedad tales como el ciudadano, la empresa privada, entes externos, etc., son actores fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas del contexto, determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público y aporte a la sociedad.

Se tienen en cuenta dentro del análisis de riesgos lo definido por el MIPG, frente a la necesidad de adelantar procesos de mejoramiento continuo y donde las oficinas de control interno permiten identificar incumplimientos y adelantar una introspección del que hacer

de la entidad desde un punto de vista objetivo. Se tienen en cuenta los hallazgos encontrados por la Oficina de Control Interno respecto a la auditoría de Seguridad de la Información buscando que se de gestión a los hallazgos encontrados dentro de dicho ejercicio. Siendo así, este documento permite alinear el objetivo de la Entidad, el objetivo del Sistema de Gestión de Seguridad de la información aunados en una gestión de riesgos que permita la mitigación de estos de cara a la seguridad de la información de la DIMAR

Es de resaltar que se tiene en cuenta que el Sistema de Gestión de Seguridad de la Información es trasversal a todos los procesos de la entidad adoptando la política de Gestión de Riesgos y enfocándola a la Seguridad de la Información tal como lo plantea el Plan Estratégico de Tecnologías de la Información – PETI 2020-2024 y las recomendaciones del reporte de Ciberseguridad para América Latina y el Caribe adelantado por la OEA y el BID[2]

7. ACTIVIDADES A DESARROLLAR

El Plan definido da cumplimiento a las actividades asociadas a la gestión del Plan de tratamiento de riesgos 2022 para la Dirección General Marítima DIMAR.

El detalle de las actividades a realizar, tiempo de ejecución de estas, responsable y participantes, para adelantar la implementación de este plan se definen a continuación.

[2] Banco Interamericano de Desarrollo. Ciberseguridad. riesgos, avances y el camino a seguir en américa latina y el caribe. 2020. Washington D.C.

ID	Nombre Actividad/Tarea	Responsable	2022
			ENE FEB MAR ABRI MAY JUN JUL AGO SEP OCT NOV DIC
		Semana	1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4
1.	**VALORACIÓN DE RIESGOS DE SEGURIDAD DIGITAL PARA SU TRATAMIENTO**		
1.1	Revisar y/o actualizar la Metodología de Riesgos de Seguridad Digital 2022	Contratista de Seguridad de la Información	
1.2	Revisar la Matriz de Activos de Información de la DIMAR 2022 (Debe estar 100% diligenciada y aprobada	Contratista de Seguridad de la Información	
1.3	Analizar, Identificar y valorar los riesgos de Seguridad y Privacidad de la Información en la Matriz, implementar los mapas de calor y ponderaciones.	Contratista de Seguridad de la Información	
1.4	Revisión de la matriz de riesgos consolidada para realizar el tratamiento de los riesgos	Contratista de Seguridad de la Información. Planeación	

ID	Nombre Actividad/Tarea	Responsable	2022
			ENE FEB MAR ABRI MAY JUN JUL AGO SEP OCT NOV DIC
		Semana	1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4
1.5	Validación con los procesos la adopción de la matriz de riesgos para desarrollar el tratamiento	Planeación y Contratista de Seguridad de la Información	
1.5	Aprobar y Divulgar	Planeación y Contratista de Seguridad de la Información	
2. CONSTRUCCIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS 2022			
2.1	Revisar y conocer marco conceptual, técnico y legal	Contratista Seguridad de la Información	
2.2	Elaborar los planes	Contratista Seguridad de la Información	
2.3	Presentación	Contratista Seguridad de la Información	

ID	Nombre Actividad/Tarea	Responsable	2022
			ENE FEB MAR ABRI MAY JUN JUL AGO SEP OCT NOV DIC
		Semana	1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4
2.4	Ajustar	Contratista Seguridad de la Información	
2.5	Publicar	Contratista Seguridad de la Información	
3. Reuniones de Seguimiento de Seguridad de la Información y Riesgos			
3.1	Reuniones de Seguimiento	Contratista Seguridad de la Información	