CONTENIDO

1. OBJETIVO 2
2. ALCANCE 2
3. GLOSARIO 2
4. DESARROLLO 4
   4.1. Cronograma de ejecución del Plan 4
   4.2. Seguimiento y Control del Plan 5
   4.3. Indicadores del Plan 5

1. OBJETIVO

Definir las actividades y tiempos con las cuales se busca avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI de la Dirección General Marítima en la vigencia 2023.

2. ALCANCE

La formulación y ejecución de este plan está liderada por el líder de seguridad de la información de la Entidad, el cual hace parte del Grupo de Informática y Comunicaciones; aplica para todos los procesos de Dimar en sede central y Unidades Regionales. Este plan tiene alcance a todos los procesos de la Entidad.

3. GLOSARIO

Activo de información: se refiere a cualquier información o elemento que tiene valor estratégico para los procesos de negocio de la Entidad. (Sistemas, soportes, edificios, hardware, recurso humano).
2
Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del Sistema de Gestión de Seguridad de la Información - SGSI de una organización.

Confidencialidad: Propiedad que garantiza que la información no sea accedida, ni sea revelada a personas, Entidades o procesos no autorizados.

Control: Toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas y que pueden ser de carácter administrativo, técnico o legal. En la entidad se aplica por medio de la declaración de aplicabilidad.

Datos: Corresponde a los elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la DIMAR.

Disponibilidad: Principio que garantiza que la información esté accesible y utilizable cuando lo requieran las personas, Entidades o procesos autorizados.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente de seguridad de la información: Violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita. Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información, tales como, un acceso no autorizado o intento del mismo; uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos.

Integridad: Principio que garantiza que la información sea exacta, coherente y completa desde su creación hasta su destrucción.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

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.

MSPI: Modelo de seguridad y privacidad de la Información.

Plan de tratamiento de riesgos (Risk treatment plan): Documento (orientado por el Decreto 612 de 2018[1]) de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la información de la Entidad.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Principios de Seguridad de la información: Confidencialidad, Disponibilidad e Integridad.

Responsable de activo de información: Persona idónea de la Entidad, que tiene la responsabilidad de adelantar acciones para que la información cumpla con los tres principios de la seguridad (Confidencialidad, Integridad y Disponibilidad).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la Información: Consiste en resguardar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja la Entidad, mediante un conjunto de medidas preventivas y correctivas.

[1] Integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. Presidencia de la República. 2018

SGSI: Sistema de Gestión de Seguridad de la Información.

Usuarios: Personas que, directa o indirectamente, tengan algún tipo de relación con la Entidad y/o que tengan acceso a los recursos tecnológicos de la Entidad, por ejemplo: funcionarios, contratistas, terceros, proveedores, entre otros.

4. DESARROLLO

4.1. Cronograma de ejecución del Plan

Tabla 1. Tareas del Plan

N°	NOMBRE DE LA TAREA	FECHA INICIAL PLANEADA	FECHA FINAL PLANEADA	RESPONSABLE
1	Formular el plan de capacitación, sensibilización y comunicación de seguridad de la información para la vigencia 2023	01-02-2023	31-03-2023	Líder de Seguridad de la información
2	Desarrollar el plan de capacitación sensibilización y comunicación de seguridad de la información para la vigencia 2023 mediante actividades: CIR, campañas, charlas, boletines informativos y/o cualquier otro mecanismo de difusión de la información.	01-02-2023	30-09-2023	Líder de Seguridad de la información
3	Revisar y/o actualizar los documentos asociados al MSPI.	01-02-2023	10-12-2023	Líder de Seguridad de la información
4	Realizar el inventario de activos de información con procesos misionales – Fase II (procesos misionales y de apoyo priorizados).	01/02/2023	15-12-2023	Líder de Seguridad de la información
5	Efectuar medición trimestral de los indicadores asociados a la matriz MSPI para la correspondiente vigencia.	01/02/2023	10-12-2023	Líder de Seguridad de la información
6	Presentar resultados del MSPI de la vigencia 2023 ante la Dirección General.	10-09-2023	10-12-2023	Líder de Seguridad de la información
7	Programar y efectuar ejercicios de simulación y respuesta a ataques cibernéticos	10-09-2023	30-11-2023	Líder Área de Plataformas, Redes y Seguridad Informática.
8	Elaborar reporte trimestral de vulnerabilidades de aplicativos y portal Web.	01-02-2023	20-12-2023	Líder Área de Plataformas, Redes y Seguridad Informática.

4.2. Seguimiento y Control del Plan

El seguimiento y control del plan se efectuará mediante el seguimiento al contrato asignado para el profesional/especialista en Seguridad de la Información, por medio de la presentación de informes de gestión y de supervisión mensuales; así como el cumplimiento de las actividades en el aplicativo SIMEC.

4.3. Indicador 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.

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