CONTENIDO

1. OBJETIVOS 2
2. ALCANCE 2
3. GLOSARIO 3
4. DESARROLLO 6
4.1. Cronograma de ejecución del Plan 6
4.2. Seguimiento y Control del Plan 8
4.3. Indicadores del Plan 8

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Definir las actividades y tiempos con las cuales se busca avanzar en la implementación del Sistema de Gestión de Seguridad de la Información de la Dirección General Marítima - Dimar en la vigencia 2022.

Tabla 1.
Objetivos específicos del plan

OBJETIVO	ACTIVIDAD	META
Identificar y priorizar los controles, políticas, procedimientos, riesgos y la capacitación o concientización de funcionarios, tendientes a la implementación del Sistema de Gestión de Seguridad de la Información	N/A	N/A
Definir un cronograma que permita la implementación de los controles, políticas, procedimientos, riesgos y la capacitación o concientización de funcionarios, con mayor prioridad e impacto dentro del Sistema de Gestión de Seguridad de la Información.	N/A	N/A
Monitorear el cumplimiento y avance de la implementación de los controles, procedimientos, políticas, riesgos, etc., del Sistema de Gestión de Seguridad de la Información, dentro de la vigencia 2022.	N/A	N/A

2. ALCANCE

Teniendo como objetivo primordial la protección de todos los activos de información, especialmente la información física y electrónica que la Entidad produzca, gestione y almacene a través de la implementación de controles físicos y lógicos que estén apuntando al cumplimiento a lo definido en numerales de la norma ISO 27001:2013. La anterior va a permitir adelantar una gestión efectiva de riesgos y un proceso de mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos previamente identificados por la Entidad.

En ese sentido, este documento busca dar un marco de trabajo que permita planear la ejecución anualizada y pormenorizada de las actividades que se pretenden adelantar para la vigencia 2022, permitiendo buscar la efectividad de las actividades y que el impacto sea el óptimo frente a las actividades elegidas sobre la implementación del SGSI.

Asimismo, también se consideran los hallazgos identificados en la pasada auditoría realizada al SGSI de la DIMAR durante el segundo semestre del 2021 por parte del Grupo de Control Interno, buscando que se den tratamiento a los mismos, e implementar acciones de mejora para las recomendaciones dadas.

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).

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.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización - tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma ISO 27001

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

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

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002[1]], es el proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

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.

[1] Guía para la administración de riesgos en seguridad de la información. DNP. 2016.

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[2]) 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 ejes 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.

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

Servicio: Cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

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.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4. DESARROLLO

4.1. Cronograma de ejecución del Plan

Tabla 2.
Tareas del Plan

N°	NOMBRE DE LA TAREA	FECHA INCIAL PLANEADA	FECHA FINAL PLANEADA	RESPONSABLE
1	Definir RTO (Recovery Time Objective o Tiempo Objetivo de Recuperación) y RPO (Recovery Point Objective u Objetivo de Punto de Recuperación) por activos, tiempo objeto de recuperación de la información.	1/04/2022	30/09/2022	Líder de Seguridad y Privacidad de la información -OSI
2	Realizar el levantamiento de activos de información con los procesos misionales	1/01/2022	30/11/2022	Líder de Seguridad y Privacidad de la información -OSI
3	Revisar y analizar la matriz actual de activos de información de la DIMAR	1/01/2022	30/09/2022	Líder de Seguridad y Privacidad de la información -OSI
4	Analizar y valorar los riesgos para los activos de información de acuerdo con el levantamiento de activos de los procesos misionales	1/01/2022	30/09/2022	Líder de Seguridad y Privacidad de la información -OSI
5	Realizar campañas de sensibilización en riesgo de seguridad de la información y seguridad informática	1/01/2022	30/06/2022	Líder de Seguridad y Privacidad de la información -OSI
6	Programar y efectuar ejercicios de simulación y respuesta a ataques cibernéticos, en coordinación con el área de infraestructura, redes y seguridad informática	1/01/2022	30/06/2022	Líder de Seguridad y Privacidad de la información -OSI
7	Efectuar evaluaciones de vulnerabilidades informáticas en coordinación con el área de infraestructura, redes y seguridad informática	1/01/2022	30/06/2022	Líder de Seguridad y Privacidad de la información -OSI
8	Definir y documentar Riesgos de Seguridad de la Información 2022	21/01/2022	30/06/2022	Líder de Seguridad y Privacidad de la información -OSI
9	Hacer seguimiento a procesos de uso de guía para la identificación de infraestructura critica cibernética	21/01/2022	30/06/2022	Líder de Seguridad y Privacidad de la información -OSI
10	Presentar a la alta dirección el protocolo estandarizado para la armonización y protección de datos personales (seguridad y privacidad).	1/04/2022	20/06/2022	Líder de Seguridad y Privacidad de la información -OSI

N°	NOMBRE DE LA TAREA	FECHA INCIAL PLANEADA	FECHA FINAL PLANEADA	RESPONSABLE
11	Realizar la revisión gerencial del Sistema de Gestión de Seguridad de la Información.	01/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
12	Elaborar el manual de activos de información (Gestión de activos - Matriz MSPI)	01/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
13	Elaborar el procedimiento de activos de información (Gestión de activos- Matriz MSPI)	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
14	Actualizar Plan de Recuperación de Desastres Tecnológicos – DRP (Matriz MSPI- Aspectos de seguridad de la información)	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
15	Elaborar el procedimiento de activos de información (Matriz MSPI- Aspectos de seguridad de la información)	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
16	Realizar informe de roles y responsabilidades para la gestión de incidentes de seguridad de la información de acuerdo con procedimientos documentados. (Gestión de incidentes de seguridad –Matriz MSPI	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
17	Actualizar procedimiento de plan de recuperación de desastres aterrizado al componente tecnológico. Gestión de incidentes de seguridad –Matriz MSPI	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
18	Gestionar los indicadores de seguridad de la información del proceso	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
19	Presentar documentación de la alienación del MSPI con el SGI	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
20	Elaborar Plan de Comunicación, Sensibilización y Capacitación en Seguridad de la Información para DIMAR	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI

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.

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.

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 y Privacidad de la información - OSI	Porcentaje (%)	Avance Actual Entidad: % Planificación del MSPI + % Implementación MSPI + % Evaluación desempeño del MSPI + %Mejora continua MSPI