TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el presente documento, se pretenden abordar los conceptos generales y repasar los controles definidos por norma ISO 27000:2013, y de esta forma definir un cronograma de trabajo, que permita la implementación de la seguridad de la información a partir de los diferentes controles, políticas, procedimientos, riesgos y la capacitación o concientización a todos y cada uno de los funcionarios y contratistas de la Dimar, buscando cumplir la declaración de aplicabilidad definida en el sistema.

Con la presentación de este plan se da cumplimiento a lo establecido en el Decreto 612 de 2018 en lo que respecta a la integración de los planes institucionales y estratégicos al plan de acción en el ámbito de aplicación del Modelo Integrado de Planeación y Gestión – MIPG y, por ende, la temporalidad que se va a trabajar está orientada a la vigencia 2022 dependiendo del cronograma presentado junto a la declaración de aplicabilidad.

2. OBJETIVOS

2.1. 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.

2.2. Objetivos Específicos

a. 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.

b. 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.

c. 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.

3. ALCANCE

Teniendo como objetivo primordial la protección de todos los activos de información, especialmente la información física y electrónica que la Entidad almacene produzca y gestione a través de la implementación de controles físicos y lógicos que estén apuntando al cumplimiento de los controles definidos en numerales de la norma ISO 27001:2013. Esto 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 identificados por la Entidad, contribuyendo al cumplimiento misional de ella.

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, permitiendo buscar la efectividad de las actividades y que el impacto sea el óptimo frente a las actividades elegidas sobre la implementación del SGSI.

4. CONCEPTOS TÉCNICOS

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).

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

Aplicaciones: Corresponde al software que se utiliza para la gestión de la información.

Personal: Corresponde a todo el personal de la SDSCJ, funcionarios, contratistas, clientes, usuarios finales y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la SDSCJ.

Servicios: Corresponde a cualquier tipo de servicios interno o externo suministrados por la Entidad a una parte interesada.

Tecnología: Corresponde a los equipos, sistemas de información, procesos y procedimientos utilizados para gestionar la información y las comunicaciones.

Instalaciones: Corresponde a todos los lugares físicos y virtuales en los que se aloja información de la Entidad.

Ambiente de Producción: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios para la ejecución de las operaciones de la Entidad. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, bases de datos, programas ejecutables o compilados.

Amenaza: Según [ISO/IEC 13335-1:2004[1]): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

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.

Autorización: Proceso o procedimiento oficial, por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información o activos físicos.

Backup o copia de seguridad: Copia de respaldo de la información.

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.

Criticidad: Medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.

Custodio: Ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.

[1] Information technology — Security techniques — Management of information and communications technology security

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.

Desviación (Seguridad de la Información): Malas prácticas adelantadas por las personas y que generan posibles incidentes o riesgos.

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

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Encriptación: Proceso que permite volver ilegible la información que se considera importante. Una vez la información esta encriptada solo puede accederse aplicando una clave.

Evaluación de riesgos: Según [ISO/lEC Guía 73:2002[2]], es el proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Excepciones (Seguridad de información): Casos especiales que no cumplen una política, procedimiento o regla.

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

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

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.

Información confidencial: Información, restringida o secreta, que es extremadamente sensible y únicamente puede ser conocida por personas específicas dentro de la Entidad. Para compartir esta información con terceros debe existir autorización expresa (escrita) de las directivas de la Entidad. Toda la información definida como reserva bancaria será clasificada como Confidencial

Infraestructura de procesamiento de información: Cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

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.

Plan de tratamiento de riesgos (Risk treatment plan): Documento (orientado por el Decreto 612 de 2018[3]) 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.

Propietario/responsable de la información: Individuo, Entidad o unidad de negocio que tienen bajo su responsabilidad la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información. Los propietarios de la información deben garantizar la seguridad, integridad, disponibilidad y confidencialidad de la información y deben coordinar la implementación de políticas con

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

otros propietarios de información y con propietarios de infraestructura. Los propietarios deben especificar cómo se debe utilizar la información y como se debe proteger, además de definir cómo se administrarán los procedimientos de control y cómo se aplicarán los niveles apropiados de protección para la información acorde con su clasificación (Pública, Pública Clasificada y Pública Reservada).

Propietarios de infraestructura: Administradores de recursos tecnológicos utilizados para el manejo y/o administración de la información. Son responsables por la funcionalidad, operación, continuidad, manejo y uso de todos los sistemas compartidos, las redes, el soporte y el mantenimiento, el software estándar, los sistemas telefónicos y de comunicaciones, y los servicios relacionados. Los propietarios de infraestructura son responsables de coordinar los servicios de recuperación de los elementos de tecnología informática y de implementar y manejar efectivamente las funciones y procedimientos de seguridad para cumplir con las necesidades de los propietarios de la información y de la Entidad.

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).

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.

Sensibilidad: Nivel de impacto que una divulgación no autorizada podría generar.

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.

Soportes físicos: Documentos en soporte físico (cartas, informes, normas, contratos) y en medios de almacenamiento físico.

Software base: Listado de software definido para ser instalado al entregar un computador. Dicho listado es definido por la Dirección de Tecnologías y Sistemas de la Información y planteado como aplicaciones mínimas para adelantar las funciones dentro de la entidad.

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

Terceros: Toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

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 [ISOIlEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5. MARCO NORMATIVO

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

6. JUSTIFICACIÓN

De acuerdo con el desarrollo del Sistema de Gestión de Seguridad y Privacidad de la Información SGSI de la Dirección General Marítima, se tiene la necesidad de definir este documento, que busca dar las pautas de desarrollo del SGSI durante el periodo 2022, buscando dar cumplimiento a la declaración de aplicabilidad definida dentro del sistema y las observaciones de Seguridad de la Información dadas por la Auditoria realizada al sistema.

De esta manera, también se toman los hallazgos y las recomendaciones dadas por la auditoría realizada al SGSI de la DIMAR durante el segundo semestre del 2021, buscando que se den tratamiento 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 de la entidad.

7. ACTIVIDADES A DESARROLLAR

El detalle de las actividades a realizar, tiempo de ejecución de las mismas, responsable y participantes, para adelantar la implementación de este plan se puede referenciar a continuación:

Nombre de la Tarea	Fecha Inicial Planeada	Fecha Final Planeada	Gestor de la Tarea
Definir RTO (*Recovery Time Objective* o Tiempo Objetivo de Recuperación) y RPO (R*ecovery 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
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
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
Analizar y valorar los riesgos para los activos de información de acuerdo al levantamiento de activos de los procesos misionales	1/01/2022	30/09/2022	Líder de Seguridad y Privacidad de la información -OSI
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
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
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

Definir y documentar Riesgos de Seguridad de la Información 2022	21/01/2022 0:00	30/06/2022 .	Líder de Seguridad y Privacidad de la información -OSI
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
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
Realizar la revisión gerencial del Sistema de Gestión de Seguridad de la Información.	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
Elaborar el manual de activos de información (Gestión de activos- Matriz MSPI)	1/04/2022	20/09/2022	Líder de Seguridad y Privacidad de la información -OSI
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
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
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

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
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
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
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
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