Tabla de Contenido

1. INTRODUCCIÓN

La Directriz General de Seguridad y Privacidad de la Información del INVEMAR, constituye los lineamientos y compromisos compartidos en el Instituto que nos permiten actuar proactivamente ante situaciones que comprometan nuestra información. Así mismo, el Manual de Lineamientos de Seguridad y Privacidad de la Información brinda los lineamientos para que las actividades relacionadas con la seguridad de la información se realicen de manera estandarizada, sistemática y organizada, con el propósito de cumplir los objetivos de seguridad del Instituto.

2. OBJETIVO

Esta directriz está dirigida a todos los trabajadores del INVEMAR, que tienen responsabilidad con el uso y/o administración de los recursos informáticos institucionales (equipos, software, sistemas de información, bases de datos, conectividad, controles de acceso, etc.). Entre los objetivos trazados tenemos:

a. Proteger, preservar y administrar objetivamente la información del Instituto junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

b. Mantener la Directriz General de Seguridad y Privacidad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos del Instituto para asegurar su permanencia y nivel de eficacia.

c. Definir las directrices del Instituto para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

3. ALCANCE

Esta directriz es de aplicación en todas dependencias del Instituto, a sus recursos, a la totalidad de los procesos internos o externos vinculados a través de contratos o acuerdos con terceros y

a todo el personal del INVEMAR, cualquiera sea su situación contractual, la dependencia en la cual se encuentre y el nivel de las tareas que desempeñe.

4. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del instituto y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: es un documento en el que los trabajadores del INVEMAR manifiestan su voluntad de mantener la confidencialidad de la información del Instituto, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Confidencialidad: Aseguramiento de que la información es accesible sólo para quienes están autorizados.

Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.

Información: Datos relacionados que tienen significado para la organización.

Integridad: Salvaguardia de la exactitud y completitud de la información y sus métodos de procesamiento.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

5. PRINCIPIOS DE SEGURIDAD QUE SOPORTAN UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

A continuación se mencionan los 12 principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información SGSI para el Instituto:

1. El INVEMAR adoptará y pondrá en práctica algunas de las normas establecidas por la ISO 27001:2013 que le darán valor agregado a las operaciones del Instituto, soportado en lineamientos claros, alineados a la misión institucional y a los requerimientos regulatorios.

2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los directivos, trabajadores, contratistas, estudiantes y proveedores del INVEMAR.

3. El INVEMAR protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros o como resultado de un servicio interno en outsourcing.

4. El INVEMAR protegerá la información generada, procesada o resguardada por los procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta información. Para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. El INVEMAR protegerá su información de las amenazas originadas por parte sus trabajadores, contratistas, estudiantes y proveedores.

6. El INVEMAR protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. El INVEMAR controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. El INVEMAR implementará control de acceso a la información, sistemas y recursos de red.

9. El INVEMAR garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. El INVEMAR garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. El INVEMAR garantizará la disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

12. El INVEMAR garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6. DIRECTRIZ GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto de Investigaciones Marinas y Costeras “José Benito Vives de Andréis” - INVEMAR, Corporación Civil sin ánimo de lucro regida por las normas del derecho privado y en especial por sus Estatutos internos, vinculada al Ministerio de Ambiente y Desarrollo Sostenible. Es consciente de la importancia de una adecuada gestión de la información para el desarrollo y buen funcionamiento de sus procesos internos, por ello, se ha comprometido con la

implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma Internacional ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información (MSPI), de Gobierno Digital, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos y establecer hacia el interior del Instituto una cultura de calidad operando en una forma confiable.

El Director, Subdirectores, Coordinadores, Jefes de Área, Profesionales y Auxiliares o cual fuere su nivel jerárquico, son responsables de la implementación de esta Directriz dentro de sus áreas, así como de su cumplimiento.

7. COMPROMISO DE LA DIRECCIÓN GENERAL

La Dirección General de INVEMAR aprueba esta Directriz General de Seguridad y Privacidad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de lineamientos eficientes que garanticen la seguridad de la información del Instituto.

La Dirección General del Instituto demuestran su compromiso a través de:

a. La revisión y aprobación de esta Directriz.
b. La promoción activa de una cultura de seguridad.
c. Facilitar la divulgación de este documento a todos los trabajadores del Instituto.
d. El aseguramiento de los recursos adecuados para implementar y mantener los lineamientos de seguridad de la información.
e. La verificación del cumplimiento de los lineamientos aquí mencionados.

8. ROLES Y RESPONSABILIDADES

La Directriz General de Seguridad y Privacidad de la Información es de aplicación obligatoria para todo el personal del Instituto, cualquiera sea su vinculación contractual, la dependencia en la cual se encuentre y el nivel de las tareas que desempeñe.
Las directivas institucionales que aprueban esta Directriz son responsables de la autorización de sus modificaciones.

ROL	RESPONSABILIDAD
Comité Institucional de Gestión y Desempeño.	✓ Coordinar la implementación de la Directriz General de Seguridad al interior del Instituto. ✓ Revisar los diagnósticos del estado de la seguridad de la información del Instituto. ✓ Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos del Instituto. ✓ Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

	✓ Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos. ✓ Promover la difusión y sensibilización de la seguridad de la información dentro del Instituto. ✓ Definir las estrategias de capacitación en materia de seguridad de la información al interior del Instituto. ✓ Impulsar la implementación de la presente Directriz. ✓ Las demás funciones inherentes a la naturaleza del Comité.
Grupo de Sistemas y Telemática	✓ Operación y supervisión del cumplimiento de la presente Directriz. ✓ Seguir los lineamientos de la presente Directriz y cumplir con los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología del Instituto. ✓ Realizar el levantamiento del inventario de activos de información y servicios tecnológicos.
Propietarios de los activos de información.	✓ Documentar y mantener actualizada la clasificación dada a sus activos, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencias. ✓ Mantener íntegro, confidencial y disponible el activo de información mientras que es mantenido y utilizado.
Coordinador de Talento Humano	✓ Notificar a todo el personal que se vincula laboralmente con el Instituto, de las obligaciones respecto al cumplimiento del MN-SYT-1 Manual de Lineamientos de Seguridad y Privacidad de la Información y de los procesos y procedimientos que surjan de éste a través del Contrato Laboral que firma con el Instituto.
Jefe Oficina Jurídica	✓ Adelantar las acciones legales pertinentes para hacer cumplir los lineamientos establecidos en la presente Directriz cuando a ello hubiere lugar. ✓ Asesorar en materia legal al Instituto en lo que se refiere a la seguridad de la información.
Auditor Interno	✓ Practicar auditorías periódicas sobre los sistemas y actividades vinculadas con los activos y la seguridad de información.

	✓ Informar sobre el cumplimiento de las especificaciones y medidas de seguridad establecidas en el Manual de Lineamientos de Seguridad y Privacidad de la información, procedimientos y prácticas que de él surjan. ✓ Garantizar que se realicen revisiones periódicas al Sistema de Gestión de Seguridad de la Información, según el procedimiento de Auditorías Internas, para verificar su vigencia, su correcto funcionamiento y su efectividad.

Nombre	Cargo
Elaborado por: Constanza Soler	Auxiliar Sistemas y Telemática (SYT)
Revisado por: Raúl Carrera Sandra Díaz Ana Milena Saade Sandra Rincón Cabal	Coordinador SYT Coordinador TAL (E) Jefe Oficina Jurídica Subdirectora Administrativa
Aprobado por: Francisco Armando Arias Isaza	Director General
Fecha de aprobación (aplica para copias emitidas desde la Oficina de Planeación)	13-08-2018