Contenido

1. INTRODUCCIÓN

La Directriz General de Seguridad y Privacidad de la Información del INVEMAR, aporta lineamientos y compromisos que permiten actuar proactivamente ante situaciones que comprometan la información institucional. Así mismo, el MN-SYT-1 Manual de Lineamientos de Seguridad y Privacidad de la Información acoge las directrices para que las actividades de gestión de seguridad y privacidad de la información se realicen de manera estandarizada,sistemática y organizada, con el propósito de cumplir los objetivos de seguridad del Instituto.

2. OBJETIVOS

Esta directriz está dirigida a todos los trabajadores de INVEMAR, que tienen responsabilidad en 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 la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

b. Mantener los lineamientos trazados en el Manual de Seguridad y Privacidad de la Información alineados con la Directriz 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 lineamientos institucionales para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información, 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 aplica a 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 de INVEMAR, cualquiera sea su situación contractual, la dependencia en la cual se encuentre y las tareas que desempeñe.

4. PRINCIPIOS DE SEGURIDAD QUE SOPORTAN LA GESTIÓN

A continuación, se mencionan los principios de seguridad que soportan la gestión de seguridad de la Información en el Instituto:

1. INVEMAR define, implementa, opera y mejora de forma continua la gestión de seguridad y privacidad de la información, soportada en lineamientos claros, alineados con la misión institucional y con 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. INVEMAR protegerá la información generada, procesada y resguardada por los procesos del negocio, su infraestructura tecnológica y los activos, del riesgo que se

genera con los accesos otorgados a terceros o como resultado de un servicio interno en outsourcing.

4. INVEMAR protegerá la información generada, procesada y resguardada por los procesos del negocio, con el fin de minimizar impactos financieros, operativos y legales, derivados de su uso incorrecto. Para ello, es fundamental la aplicación de controles que consideren la clasificación de la información propia o en custodia.

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

6. INVEMAR protegerá las instalaciones de procesamiento y la infraestructura tecnológicaque soporta sus procesos críticos.

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

8. INVEMAR implementará controles de acceso a la información y a los sistemas y recursos de red.

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

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

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

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

5. POLÍTICA GLOBAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto de Investigaciones Marinas y Costeras “José Benito Vives de Andréis” - INVEMAR, es una 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. INVEMAR 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 a establecer loslineamientos necesarios para garantizar la seguridad y privacidad de la información y a regular la gestión de la seguridad cumpliendo con los requisitos de seguridad, estableciendo un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos y, creando una cultura de calidad.

El director, subdirectores, coordinadores, jefes de área, profesionales y auxiliares son responsables de la implementación y cumplimiento de esta Directriz en sus correspondientes áreas.

6. COMPROMISO DE LA DIRECCIÓN GENERAL

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

7. 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.

A continuación, se establecen los roles y responsabilidades que darán cumplimiento a la presente Directriz y en el Anexo 1 – DZ-SYT-1 Roles y Cargos Equipo de Gestión de Seguridad y Privacidad de la información y Plan Estratégico de Tecnologías de la Información PETI, se definen los cargos por rol para atender las responsabilidades definidas.

ROL	RESPONSABILIDAD
Alta Dirección	✓ Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad. ✓ Revisar los diagnósticos del estado de la seguridad y privacidad de la información del Instituto. ✓ Acompañar e impulsar el desarrollo de proyectos de seguridad. ✓ 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 y privacidad de la información. ✓ Promover la difusión y sensibilización de la seguridad y privacidad de la información en el Instituto. ✓ Poner en conocimiento del Instituto, los documentos generados al interior en temas de seguridad que impacten de manera transversal a la misma.
Comité Institucional de Gestión y Desempeño.	✓ Coordinar la implementación de la DirectrizGeneral de Seguridad al interior 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. ✓ Adoptar el uso de metodologías y procesos específicos para la seguridad de la información emitidos por MINTIC y DAFP. ✓ Promover la difusión y sensibilización de laseguridad de la información dentro del Instituto. ✓ Promover 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.

ROL	RESPONSABILIDAD
Planeación	✓ Vigilar que las acciones y mejoras propuestas en torno a los temas de seguridad y privacidad de la información estén alineadas con los lineamientos estratégicos del INVEMAR. ✓ Acompañar al Grupo de Sistemas y Telemática y Laboratorio de Servicios de Información en las sesiones para la construcción del PETI conforme lo establece el MINTIC. ✓ Asesorar a la al Grupo de Sistemas y Telemática y al Laboratorio de Servicios de Información en los aspectos generales de la gestión de riesgos y todas aquellas que sean de su competencia relacionadas con el direccionamiento estratégico del INVEMAR.
Gestor MSPI	✓ Planear, ejecutar, verificar y realizar seguimiento a la implementación de la seguridad y privacidad de la información. ✓ Elaborar, promover y mantener actualizada la Directriz de Seguridad y Privacidad de la Información y el Manual de Lineamientos de Seguridad y Privacidad de la información. ✓ Realizar el levantamiento del inventario de activos de información y servicios tecnológicos. ✓ Identificar la brecha entre el Sistema de Gestión de Seguridad de la Información SGSI y la situación del Instituto, aportando oportunidades de mejora que permitan alcanzar la implementación en el futuro de este sistema. ✓ Generar cronograma de actividades orientadas a mejorar la seguridad y privacidad de la información en el Instituto. ✓ Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto. ✓ Realizar las revisiones periódicas del cumplimiento a los temas de seguridad y privacidad de la información.
Líder Estratégico de TI	✓ Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo. ✓ Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar de ser necesario al Comité de Gestión y Desempeño Institucional. ✓ Operar y supervisar el cumplimiento de la presente Directriz y lo contemplado en el documento MN-SYT-1 Manual de Lineamientos de Seguridad y Privacidad de la Información. ✓ 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.

ROL	RESPONSABILIDAD
	✓ Definir los controles necesarios para mitigar los riesgos de seguridad que se identifiquen. ✓ Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido. ✓ Facilitar la administración y desarrollo de iniciativas sobre seguridad de información en el Instituto. ✓ Proveer dirección y experiencia técnica para asegurar que la información se encuentre protegida apropiadamente. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan. ✓ Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y estable de recursos de información que sea consistente con las metas y objetivos del Instituto. ✓ Revisar el estado de la seguridad y privacidad de la información. ✓ Revisar y analizar los incidentes de seguridad suscitados en el Instituto, es decir incidentes de seguridad con impacto alto, considerados como severos. ✓ Identificar necesidades de evaluación de procesos soportados por recursos informáticos y su plataforma tecnológica. ✓ Avalar y aprobar la ejecución de proyectos de seguridad de información (pe. adquisición de soluciones.). ✓ Servir de facilitadores para el desarrollo de proyectos de seguridad y privacidad de información. ✓ Validar las directrices de seguridad y privacidad de la información o las modificaciones a las mismas. ✓ Cumplir con las políticas de seguridad de la información establecidas para la infraestructura tecnológica. ✓ Contratar los recursos necesarios para garantizar la seguridad física de las instalaciones y la información. ✓ Cumplir con las políticas de seguridad y privacidad de la información establecidas para el desarrollo de software interno y externo. ✓ Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos. ✓ Establecer controles de seguridad de la información con el fin de prevenir riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información.
Propietarios de los activos de información.	✓ Documentar y mantener actualizada la clasificación dada a sus activos, definiendo los usuarios con permiso de acceso a la información, de acuerdo con sus funciones y competencias. ✓ Mantener íntegro, confidencial y disponible el activo de información mientras es mantenido y utilizado. ✓ Adoptar el uso de metodologías y procesos específicos para la seguridad de la

ROL	RESPONSABILIDAD
	información. ✓ Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos de sus activos de información.
Talento Humano	✓ Notificar a todo el personal que se vincula laboralmente con el Instituto, de las obligaciones sobre el cumplimiento del documento MN-SYT-1 Manual de Lineamientos de Seguridad y Privacidad de la Información y sobre los procesos y procedimientos que surjan de éste a través del contrato laboral que se firma. ✓ Verificar que en los contratos laborales queden las cláusulas de confidencialidad y sean comprendidas. ✓ Socializar los lineamientos de tratamiento de datos personales que se estipula en el INVEMAR. ✓ Velar por que todos los trabajadores vinculados que hagan uso de la información del Instituto, den cumplimiento a los lineamientos contenidos en el MN-SYT-1 Manual de Lineamientos de Seguridad y Privacidad de la Información. ✓ Garantizar la capacitación y competencia del Talento Humano para la gestión de seguridad y privacidad de la Información. ✓ Promover que el personal vinculado laboralmente cuente con un nivel de conciencia en seguridad y privacidad de la información para la correcta gestión de los activos de información. ✓ Asegurar que los procesos de desvinculación, licencias, vacaciones o cambio de cargo de los trabajadores del Instituto sean debidamente gestionados en todo lo concerniente a permisos o cambios en los accesos a la plataforma tecnológica del Instituto con el apoyo de la Coordinación de Sistemas y Telemática.
Gestión Contractual	✓ Notificar a todo el personal que se vincula contractualmente con el Instituto, de las obligaciones sobre el cumplimiento del documento MN-SYT-1 Manual de Lineamientos de Seguridad y Privacidad de la Información y sobre los procesos y procedimientos que surjan de éste a través del contrato que se firma. ✓ Verificar que el personal provisto por prestación de servicios firme y garantice el cumplimiento de la cláusula de confidencialidad y uso restringido de la información estipulado en el contrato de servicios, antes de otorgarles acceso a la información. ✓ Verificar que en los contratos laborales queden cláusulas de confidencialidad y sean comprendidas. ✓ Verificar que en sus contratos con proveedores o terceros incluyan los Acuerdos de Niveles de Servicio (ANS) para los procesos de tecnología y cumplir con los requisitos de seguridad y privacidad de la información dispuestos en el MN-SYT-1 Manual de Lineamientos de Seguridad y Privacidad de la Información.

ROL	RESPONSABILIDAD
Oficina Jurídica	✓ Verificar el cumplimiento de la presente Directriz. ✓ Asesorar en materia legal al Instituto en lo que se refiere a la seguridad de la información. ✓ Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales. ✓ Tramitar las consultas, solicitudes y reclamos. ✓ Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran. ✓ Respetar las condiciones de seguridad y privacidad de información del titular. ✓ Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente. ✓ Servir como apoyo para analizar, asesorar, conceptuar y orientar sobre los datos que son susceptibles de poner a disposición de cualquier persona, sin que esto implique la vulneración de los derechos fundamentales de los individuos y el incumplimiento de la normatividad, en cuanto a respetar la reserva legal que tienen algunos datos o información. ✓ Identificar y mantener actualizado el normograma de seguridad y privacidad de la información.
Auditoria Interna	✓ 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 definidas en el documento MN-SYT-1 Manual de Lineamientos de Seguridad y Privacidad de la información, y en los procedimientos y prácticas establecidas.

5. ANEXOS

- AX-SYT-12 Roles y cargos equipo de gestión de seguridad y privacidad de la información y Plan Estratégico de Tecnologías de la Información - PETI

Nombre	Cargo
Elaborado por: Constanza Soler	Auxiliar Sistemas y Telemática (SYT)
Revisado por: Raúl Carrera Sandra Rincón Cabal	Coordinador Sistemas y Telemática Subdirectora Administrativa
Aprobado por: Francisco Armando Arias Isaza	Director General
Fecha de aprobación (aplica para copias emitidas desde la Oficina de Planeación)	2021-11-26