Contenido

INTRODUCCIÓN

El Manual de Lineamientos de Seguridad y Privacidad de la información del INVEMAR, emerge como instrumento para concientizar a sus trabajadores acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades de la red de datos, sistemas de información e infraestructura tecnológica, de tal forma que permitan al Instituto cumplir con su misión. Por ello, se hace necesario que el Instituto establezca un marco en el cual se asegure que la información que se genera es protegida adecuadamente, independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

En este contexto el Instituto de Investigaciones Marinas y Costeras – INVEMAR, debe identificar y definir los lineamientos que faciliten la gestión y la gobernabilidad de TI, alcanzando sus objetivos estratégicos, basados en un enfoque de gestión y mejora continua, donde se establezcan un conjunto de directrices específicas, que son el soporte de la Directriz General de Seguridad y Privacidad de la Información, adoptada por el Instituto.

Para esto, todas las partes interesadas que tienen responsabilidad sobre los repositorios y recursos de información del Instituto, deben adoptar los lineamientos contenidos en presente manual, así como los documentos que se encuentren relacionados con él, buscando asegurar la confidencialidad, integridad y disponibilidad de la información.

1. OBJETIVO

Establecer los lineamientos necesarios para garantizar la seguridad y privacidad de la información en el INVEMAR, con el fin de regular la gestión de la seguridad y privacidad de la información y cumplir con los requisitos de seguridad definidos por el Modelo de Seguridad y Privacidad de la Información MSPI de la Política de Gobierno Digital, que ayudarán mediante su implementación a preservar la confidencialidad, integridad y disponibilidad de la información al interior del Instituto, mejorando la calidad de los servicios.

2. ALCANCE

Los lineamientos de seguridad y privacidad de la información, contenidos en este manual, serán aplicados a los procesos gerenciales, misionales, de evaluación y de apoyo del Instituto, por tal motivo serán aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, trabajadores, contratistas, estudiantes y proveedores, que accedan a sus sistemas de información, repositorios e instalaciones físicas o que presten sus servicios o tengan una relación laboral con el INVEMAR.

Adicionalmente se incluyen lineamientos de seguridad de la información para los activos que se encuentren alojados en la nube y también para las actividades de desarrollo de software ejecutadas por terceros.

3. MARCO LEGAL

- Decreto 767 de 2022 Política de Gobierno Digital. "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital".
  https://www.mintic.gov.co/portal/715/articles-210461_recurso_1.pdf

- Resolución 746 de 2022 "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.
  https://www.mintic.gov.co/portal/715/articles-208143_recurso_1.pdf

- Resolución 1519 de 2020 "Por el cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 de 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos".
  https://gobiernodigital.mintic.gov.co/692/articles-178657_resolucion_1519_2020.pdf

- Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital".
  https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

- CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital busca "Establecer medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías".
  https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

- CONPES 3854 de 2016 – Política Nacional de Seguridad Nacional, busca fortalecer, identificar, gestionar, tratar y mitigar riesgos de seguridad digital.
  https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
  https://normograma.mintic.gov.co/mintic/docs/pdf/decreto_1078_2015.pdf

- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de. Acceso a la Información Pública Nacional.
  https://normograma.mintic.gov.co/mintic/docs/ley_1712_2014.htm

- Norma Técnica Colombiana ISO 27001:2013. Específica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGI). https://serviciocivil.gov.co/sites/default/files/marco-legal/2006_03_22_NTC-ISO-IEC%2027001.pdf

- Modelo de Seguridad y Privacidad de la Información – MSPI – Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la información. https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

4. TÉRMINOS Y DEFINICIONES

Activo: Cualquier cosa que tenga valor para el Instituto.

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 mismo.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Centros de cableado: son habitaciones donde se instalan los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de ésta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

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.

Estándar: regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel del Instituto antes de crear nuevas políticas.

Evaluación de riesgos: Todo proceso de análisis y valoración del riesgo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Guías de clasificación de la información: directrices para catalogar la información de una entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Gusanos: es un programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de una entidad con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes al Instituto.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CD, DVD y unidades de almacenamiento USB, entre otras.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los

sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través del Instituto.

NTC-ISO-IEC 27001:2013: Norma Técnica: Es un estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

No repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de una entidad.

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Tecnología de la Información: Se refiere al hardware y software operados por el INVEMAR o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Instituto, sin tener en cuenta la tecnología utilizada, ya se trate de datos, telecomunicaciones u otro tipo.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a el Instituto.

Tratamiento del riesgo: Proceso de selección e implementación de medidas a para modificar el riesgo.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el Instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

5. DIRECTRIZ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1 Orientación de la Dirección para la gestión de la Seguridad y Privacidad de la Información

Objetivo: Definir, implementar, operar y mejorar 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.

5.1.1 Lineamiento para la Seguridad y Privacidad de la Información

Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.

En cumplimiento de su misión institucional "Realizar investigación básica aplicada de los recursos naturales renovables y del medio ambiente en los litorales y ecosistemas marinos y oceánicos de interés nacional, con el fin de proporcionar el conocimiento científico necesario para la formulación de políticas, la toma de decisiones y la elaboración de planes y proyectos que conduzcan al desarrollo de éstas, dirigidos al manejo sostenible de los recursos, a la recuperación del medio ambiente marino y costero y al mejoramiento de la calidad de vida de los colombianos, mediante el empleo racional de la capacidad científica del Instituto y su articulación con otras entidades públicas y privadas"; el Instituto como muestra de su compromiso y apoyo, ha diseñado he implementado lineamientos eficientes que garanticen la seguridad de la información; así mismo, se compromete a hacer uso eficiente de sus recursos, a preservar la confidencialidad, integridad y disponibilidad de la información, bajo un enfoque de prevención de riesgos, con la miras a la mejora continua en la prestación de los servicios, con el apoyo de su equipo humano capacitado, competente y comprometido.

5.1.2 Revisión de los lineamientos de Seguridad y Privacidad de la Información

Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.

El Instituto debe realiza la revisión del Manual de Lineamientos de Seguridad y Privacidad de la Información al menos una vez al año o cuando lo considere pertinente, teniendo en cuenta cambios o ajustes que surjan en el tiempo y que afecten el cumplimiento del lineamiento.

6. ORGANIZACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 Organización Interna

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la entidad.

6.1.1 Seguridad de la información Roles y Responsabilidades

Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.

- Se asignan roles y responsabilidades acuerdo a documento Anexo 1 DZ-SYT-2 Roles y Cargos equipo de gestión de seguridad y privacidad de la información y Plan Estratégico de Tecnologías de la información – PETI.

- Todos los trabajadores del INVEMAR, que tienen responsabilidad en el uso y/o administración de los recursos informáticos institucionales o que tengan acceso a información física, son responsables de cumplir los lineamientos de seguridad y privacidad de la información, descritas en este manual.
- La Coordinación de Sistemas y Telemática implementará y gestionará los controles tecnológicos necesarios que requieran para su óptima operación los sistemas de información, plataformas de apoyo o infraestructura de comunicaciones y seguridad del Instituto.
- Los propietarios de los activos de información, son responsables de establecer la identificación, valoración y clasificación de los activos, teniendo en cuenta el documento GI-SYT-3 Guía para la elaboración del inventario y la clasificación de activos de información. Así mismo, deberán mantener actualizado éste inventario, validando los controles de acceso asignados a los activos.
- Los propietarios de los activos de información, deberán identificar los riesgos de seguridad asociados a éstos y reportar oportunamente los incidentes de seguridad a los que se vean expuestos.

6.1.2 Separación de deberes

Control: Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.

- El Instituto a través del Grupo de Sistemas y Telemática garantiza que todos sus sistemas de información y plataformas en la nube cuentan con controles de acceso de manera que haya separación de funciones entre los trabajadores que las administran, las utilizan, las mantengan, las auditen y, en general que tengan opción de acceder a los sistemas de información.

6.1.3 Contacto con las autoridades

Control: Se debe mantener contactos apropiados con las autoridades pertinentes.

- El Instituto debe mantener actualizado los contactos con las autoridades competentes, tales como la Policía Nacional y el CSIRT DE Gobierno y registrar los incidentes de seguridad en el portal de la Superintendencia de Industria y Comercio en caso de ser incidentes de seguridad a los datos personales.

6.1.4 Contacto con grupos de interés especial

Control: Se debe mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

- El Instituto a través de su Coordinación de Sistemas y Telemática mantiene contacto con grupos de interés especial, foros y asociaciones profesionales especializadas en seguridad, con el fin de mantenerse actualizado en temas relacionados con seguridad y privacidad de la información.

6.1.5 Seguridad de la información en Gestión de Proyectos

Control: La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto.

- El Instituto debe establecer los lineamientos de seguridad de la información para la gestión de proyectos.

6.2 Dispositivos Móviles y Teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

6.2.1 Lineamiento para dispositivos móviles

Control: Se debe adoptar una directriz y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

- El Instituto debe establecer una directriz para el manejo de dispositivos móviles institucionales que acceden a la información del Instituto y debe velar por el uso responsable de éstos por parte de los trabajadores. Para dar cumplimiento al lineamiento se cuenta con el documento DZ-SYT-6 Directriz para Uso de Dispositivos Móviles V.1.

6.2.2 Teletrabajo

Control: Se debe implementar una directriz y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

- El Instituto establece los lineamientos a seguir para las modalidades de: Teletrabajo, Trabajo en Casa y Trabajo remoto, los cuales están contemplados en el documento RG-TAL-1 Reglamento Interno de Trabajo Artículo 87, Artículo 108 y Artículo 117.
- El Instituto provee a los trabajadores que estén en cualquiera de las modalidades de: Teletrabajo, Trabajo en Casa o Trabajo remoto, los lineamientos y mecanismos de seguridad de

la información que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

- El trabajador que labore bajo cualquiera de las modalidades de: Teletrabajo, Trabajo en Casa o Trabajo remoto, no debe ceder en ningún caso a terceras personas la información a la que tenga acceso.
- El trabajador que labore bajo cualquiera de las modalidades de: Teletrabajo, Trabajo en Casa o Trabajo remoto se compromete a cumplir con los lineamientos de seguridad descritos en este manual con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de los activos de información del Instituto.
- Para realizar labores en cualquiera de las modalidades, el trabajador deberá previamente realizar la solicitud al Grupo de Sistemas y Telemática a través de la mesa de servicios, con la finalidad de proveer los enlaces de comunicación seguros (VPN).

7. SEGURIDAD DE LOS RECURSOS HUMANOS

7.1 Antes de asumir el empleo

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

7.1.1 Selección

Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

- El INVEMAR reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantiza que la vinculación de nuevos trabajadores se realizará siguiendo el proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los trabajadores en sus cargos.

7.1.2 Términos y condiciones del empleo

Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.

- La Coordinación de Talento Humano con el apoyo de la Coordinación de Gestión Contractual garantizan que los contratos de trabajo y los contratos de prestación de servicios contengan la Cláusula de Confidencialidad debidamente diligenciada durante la vinculación de trabajadores, prestación de servicios y terceras partes.
- El INVEMAR debe promover que el personal vinculado y provisto por prestación de servicios cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan los lineamientos de seguridad y privacidad de la información en el Instituto.

7.2 Durante la ejecución del empleo

Objetivo: Asegurarse que los trabajadores, contratistas, estudiantes y pasantes tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

7.2.1 Responsabilidades de la Dirección

Control: La Dirección debe exigir a todos los trabajadores, contratistas, estudiantes y pasantes la aplicación de la seguridad de la información de acuerdo con los lineamientos y procedimientos establecidos.

- El Coordinador del Grupo de Gestión Contractual se asegurará 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.

7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Control: Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

- Los contratistas, pasantes y estudiantes del INVEMAR deben recibir educación y formación en toma de conciencia apropiada sobre seguridad y privacidad de la información; también recibirán información actualizada sobre éste tema de directrices y procedimientos a través de las inducciones de ingreso, re-inducciones generales y divulgaciones.
- La Coordinación de Sistemas y Telemática con el apoyo de la Coordinación de Talento Humano, concientizará a los trabajadores del Instituto a través de campañas de sensibilización sobre seguridad de la información para evitar posibles riesgos de seguridad.

- Todos los trabajadores del INVEMAR deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre del Instituto.
- El Instituto realiza periódicamente comunicados masivos sobre riesgos de seguridad y privacidad de la información.

7.2.3 Proceso disciplinario

Control: Se debe contar con un proceso formal comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

- Se consideran violaciones graves, el robo, daño, divulgación de información reservada o confidencial del INVEMAR, o que se le declare culpable de un delito informático. Por ello, será objeto de las sanciones que el INVEMAR tenga contempladas o las que por ley el INVEMAR deba tomar como medidas de protección de los bienes y/o información afectada y las cuales se encuentran definidas en el documento RG-TAL-1 Reglamento Interno de Trabajo.

7.3 Terminación o cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

7.3.1 Terminación o cambio de responsabilidades de empleo

Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

- Para la terminación del empleo se establece dentro del flujo de trabajo FT-TAL-20 v.2 Acta de Entrega de Cargo las aprobaciones de paz y salvo por parte de las dependencias que tienen vínculos con el trabajador y evidenciando con ésta aprobación que desde el Grupo de Sistemas y Telemática se realiza el retiro de los accesos lógicos sobre la infraestructura tecnológica y física de acuerdo con el documento DZ-SYT-4 v.2 Directriz de Control de Acceso y el documento PR-SYT-3 Procedimiento para la Administración de Cuentas de usuario.
- El Grupo de Talento Humano y el Grupo de Gestión Contractual informarán al Grupo de Sistemas y Telemática los nuevos trabajadores vinculados con la finalidad de realizar la activación de los servicios tecnológicos y dar acceso a las plataformas institucionales.

- En caso de desvinculación de algún trabajador, el Grupo de Talento Humano o Gestión Contractual informará de inmediato al Grupo de Sistemas y Telemática para realizar el retiro de los servicios tecnológicos que tenga a cargo el trabajador desvinculado.

8. GESTIÓN DE ACTIVOS

8.1 Responsabilidad por los activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.

8.1.1 Inventario de Activos

Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

- El INVEMAR cuenta con el documento MT-SYT-1 Matriz de Inventario y Clasificación de Activos de Información por proceso, donde se encuentran debidamente identificados los activos de información.
- El Instituto ha dispuesto el documento GI-SYT-3 Guía para la elaboración del Inventario y la clasificación de activos de información para el levantamiento e identificación de activos de información.
- El Instituto realiza el inventario de activos de información apoyado en las áreas o dependencias que tienen responsabilidad sobre éstos.
- Es responsabilidad de los propietarios de los activos de información, identificarlos y clasificarlos debidamente apoyados en el documento GI-SYT-3 Guía para la elaboración del Inventario y la clasificación de activos de información dispuesto en el Sistema Kawak.
- Una vez aprobados los activos de información deben ser publicados en el repositorio de información documental institucional, el Sistema Kawak.

8.1.2 Propiedad de los Activos

Control: Los activos mantenidos en el inventario deben ser propios.

- Los líderes de los procesos serán los propietarios de los activos de información.
- Cada proceso debe ser el responsable de mantener debidamente actualizado el inventario de activos de información y el líder del proceso deberá aprobar y reportar su actualización cuando haya lugar.

8.1.3 Uso aceptable de los Activos

Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

- La información, los archivos digitales, los archivos físicos, los sistemas de información, los servicios digitales y los equipos de cómputo son activos del Instituto y se proporcionan a los funcionarios, contratistas y terceros para cumplir con los propósitos misionales del INVEMAR.
- Está prohibido que trabajadores, contratistas, proveedores o terceros ajenos al Grupo de Sistemas y Telemática, destapen o retiren partes de los equipos de cómputo del INVEMAR.
- Para la instalación de cualquier tipo de software o hardware en los equipos de cómputo debe solicitar a través de la mesa de servicios del Grupo de Sistemas y Telemática, su instalación.
- Los equipos de cómputo de deben ser movidos del sitio asignado, ni trasladar a otro trabajador el equipo sin la respectiva autorización del Grupo de Sistemas y Telemática.
- No se permite realizar ninguna configuración a los equipos de cómputo por parte de los trabajadores. Estas actividades son exclusivas del Grupo de Sistemas y Telemática.
- No se autoriza el uso de medios extraíbles para almacenamiento de información institucional (USB, discos duros, tarjetas de memoria, equipos móviles, tales como tabletas o celulares), acuerdo a lo dispuesto en la directiva DR DGI-SRA-SYT 03-24 “Por la cual se acoge la disposición de prohibir el uso y almacenamiento de información institucional en dispositivos externos”.
- Los equipos de cómputo (CPU y Monitor), servidores e impresoras, debe conectarse a los puntos de corriente eléctrica naranja, los cuales son de uso exclusivo para equipos de cómputo, con el fin de evitar picos de voltaje que puedan dañar el componente tecnológico.
- La seguridad física de equipos de cómputo que ingresen y que no sean de propiedad del INVEMAR son responsabilidad exclusiva de su propietario.

8.1.4 Devolución de activos

Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

- Todos los trabajadores o contratistas que tienen a cargo activos fijos deben gestionar su devolución de sus activos que tiene a su cargo al terminar su contrato laboral, gestionando el FT-TAL-20 Acta de Entrega de Cargo.
- Todos los trabajadores o contratistas que tengan un contrato laboral con el Instituto, deben entregar toda la información producto del trabajo realizado, una vez se finalice el vínculo laboral con el Instituto.

8.2 Clasificación de la información

Objetivo: Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

8.2.1 Clasificación de la información

Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

- Los trabajadores propietarios y responsables de los activos de información deben asegurarse que los activos a su cargo se encuentren inventariados en el documento MT-SYT-3 Matriz de Inventario y Clasificación de Activos de Información por procesos e informar al Oficial de Seguridad en caso que no se encuentre inventariado, para su debida actualización y registro.
- Los propietarios de los activos de información deben clasificar sus activos de información, con base en lo descrito en la GI-SYT-3 Guía para la elaboración del inventario y la clasificación de activos de información.
- Los trabajadores responsables de los activos de información deben asegurarse de que los activos de información bajo su responsabilidad se encuentren clasificados y protegidos adecuadamente.

8.2.2 Etiquetado de la información

Control: Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

- Los activos de información se encuentran debidamente etiquetados en el documento MT-SYT-1 Matriz de Inventario y Clasificación de Activos de Información por procesos.

8.2.3 Manejo de Activos

Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información.

- Los activos de información se encuentran debidamente etiquetados en el documento MT-SYT-1 Matriz de Inventario y Clasificación de Activos de Información por procesos y apoyados en la GI-SYT-3 Guía para la elaboración del inventario y la clasificación de activos de información para su manejo y control.

8.3 Manejo de medios de soporte

Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

8.3.1 Gestión de medios de soporte removibles

Control: Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.

- El Instituto ha implementado la directriz DR DGI-SRA-SYT 03-24 "Por la cual se acoge la disposición de prohibir el uso y almacenamiento de información institucional en dispositivos externos" tales como: USB, discos duros, tarjetas de memoria, tabletas, celulares como medio de almacenamiento externo.
- El manejo de la información del Instituto en medios removibles está expuesta a riesgos, como, pérdida de información, fuga o modificación, los cuales comprometen la información y la infraestructura tecnológica del Instituto, por lo tanto, el propietario del activo de información que autorice su uso y el autorizado, asumirán las sanciones de ley aplicables en esta materia, siendo los responsables de la seguridad de uso de la información a través de éstos medios.
- El control de los medios removibles estará a cargo del propietario de los activos de información, quien realizará la solicitud de autorización de acceso y uso de puertos y mecanismos necesarios para el uso de estos dispositivos.

8.3.2 Disposición de los medios de soporte

Control: Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.

- Se debe realizar el borrado de toda la información que no se requiera o que no sea útil en los medios removibles, de tal forma que no pueda ser restaurada ni reconstruida.
- El propietario del activo de la información deberá evaluar la viabilidad de la destrucción de la información almacenada en los medios removibles de manera que ésta no pueda ser reutilizada en un espacio o lugar al motivo inicial de su disposición.

8.3.3 Transferencia de medios de soporte físicos

Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

- Se debe definir un procedimiento de intercambio seguro de información física o digital.

- Cuando se realicen convenios o acuerdos entre entidades para el intercambio de información física o digital, se debe especificar la clasificación de la información y las consideraciones de seguridad de ésta.
- Validar que el proveedor de transporte o de los servicios de mensajería realice un adecuado embalaje de la información física que es enviada.

9. CONTROL DE ACCESO

9.1 Requisitos del negocio para control de acceso

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

9.1.1 Política de Control de Acceso

Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

- El Instituto tiene definido el documento DZ-SYT-4 Directriz de Control de Acceso en donde se determina los criterios de acceso a la información a través de mecanismos de control de acceso lógico y físico y se establecen lineamientos generales para controlar el acceso a áreas seguras, reduciendo el riesgo de pérdida de información o daños a recursos.

9.1.2 Acceso a redes y a servicios en red.

Control: Sólo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

- Desde el Grupo de Talento Humano se notifica al Grupo de Sistemas y Telemática el ingreso de nuevos trabajadores al Instituto y solicitan acceso a los servicios tecnológicos a través de la mesa de servicios dispuesta para los requerimientos del área.
- El Grupo de Sistemas y Telemática se encarga de permitir el acceso a la red, de los trabajadores, contratistas, estudiantes y aprendices y notifica vía correo electrónico las credenciales de acceso a los servicios tecnológicos dispuestos para el desempeño de sus funciones.
- El INVEMAR garantiza que todos sus trabajadores, contratistas y estudiantes, que tengan necesidad de acceder a las redes o recursos de red del Instituto deben seguir los lineamientos de seguridad establecidos en este documento y en la directriz DZ-SYT-4 Directriz Control de Acceso.

9.2 Gestión de acceso de usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

9.2.1 Registro y cancelación del registro de usuarios

Control: Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.

- El INVEMAR tiene establecida la directiva DZ-SYT-4 Directriz Control de Acceso, con la finalidad de contar con un proceso formal de registro de usuarios y proteger al Instituto contra accesos no autorizados a través de mecanismos de control lógico y físico, reduciendo el riesgo de pérdidas de información o daños a recursos.
- Se realizan revisiones periódicas en los diferentes sistemas de información, aplicaciones y demás herramientas tecnológicas con la finalidad de garantizar que los usuarios que ya no se encuentran vinculados laboralmente se encuentren deshabilitados en éstos.
- El Grupo de Talento Humano, notifica a través de correo electrónico al Grupo de Sistemas y Telemática, los usuarios que han sido desvinculados al Instituto, con la finalidad de ser retirados de los sistemas de información y demás recursos que tecnológicamente fueron asignados.
- Se bloquean de manera inmediata los privilegios de acceso físico a las instalaciones del Instituto.
- El trabajador antes de retirarse debe gestionar el formato FT-TAL-20 Acta de entrega de cargo, con la finalidad que se realice la entrega formal del cargo y se evidencie el paz y salvo con las dependencias del INVEMAR con las que tuvo contacto; posteriormente, realice la entrega de los activos fijos a cargo y realizar la devolución del carnet institucional.
- El Instituto deberá implementar un procedimiento en donde se establezca el registro y cancelación de usuarios a los diferentes sistemas de información (Sistema UNOEE, Sistema Kactus, Sistema Kawak, Intranet, entre otros, etc.).

9.2.2 Suministro de acceso de usuarios

Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.

- Los Lineamientos de Administración de acceso de usuarios serán aplicados por el Grupo de Sistemas y Telemática a través de su documento PR-SYT-3 Procedimiento para la Administración de Cuentas de Usuario y de la directriz DZ-SYT-4 Directriz Control de Acceso, con el fin de establecer privilegios para el control de acceso lógico de cada usuario a través de las redes de datos, los recursos tecnológicos y los sistemas de información del Instituto. Así mismo, verificará

que los trabajadores y personal contratado por prestación de servicios, tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y por qué la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

9.2.3 Gestión de Derechos de acceso privilegiado

Control: Se debe restringir y controlar a asignación y uso de derechos de acceso privilegiado.

- La Coordinación de Sistemas y Telemática otorga los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos trabajadores designados para dichas funciones.

- La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar por parte de la Coordinación de Sistemas y Telemática, tales como: “administrador”, “system” o “root”, dejando registro de trazabilidad de uso de estos accesos.

- La Coordinación de Sistemas y Telemática restringe las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se permiten los accesos a personal autorizado, de acuerdo con las labores desempeñadas.

- La Coordinación de Sistemas y Telemática debe asegurar que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

- La Coordinación de Sistemas y Telemática establece los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

- Los administradores de los recursos tecnológicos y servicios de red, trabajadores del Grupo de Sistemas y Telemática, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica del INVEMAR.

- La Coordinación de Sistemas y Telemática genera y mantiene actualizadas las cuentas administrativas de los recursos de la plataforma tecnológica.

9.2.4 Gestión de Información de autenticación secreta de usuarios

Control: La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.

- Todos los trabajadores, contratistas, estudiantes y aprendices deben mantener estricto control y confidencialidad de la información secreta de sus credenciales (contraseñas de las cuentas de usuario y accesos a sistemas de información).

9.2.5 Revisión de los derechos de acceso de usuarios

Control: Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.

- Los Lineamientos de Administración de acceso de usuarios serán aplicados por el Grupo de Sistemas y Telemática a través de su documento PR-SYT-3 Procedimiento para la Administración de Cuentas de Usuario y de la directriz DZ-SYT-4 Directriz Control de Acceso, con el fin de establecer privilegios para el control de acceso lógico de cada usuario a través de las redes de datos, los recursos tecnológicos y los sistemas de información del Instituto. Así mismo, verificará que los trabajadores y personal contratado por prestación de servicios, tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y por qué la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

- La Coordinación de Sistemas y Telemática establece un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los trabajadores se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

- Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el encargado del Grupo de Sistemas y Telemática, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

- Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

9.2.6 Cancelación o ajuste de los derechos de acceso

Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.

- La Coordinación de Sistemas y Telemática, vela porque los recursos de la plataforma tecnológica y los servicios de red del instituto sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos servicios. Para ello, la implementado la directriz DZ-SYT-4 Directriz Control de Acceso y del procedimiento PR-SYT-3 Procedimiento para la Administración de Cuentas de Usuario, garantizando la seguridad de los recursos y servicios tecnológicos del INVEMAR.

9.3 Responsabilidades de los usuarios

Objetivo: Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.

9.3.1 Uso de información secreta para la autenticación

Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

- La Coordinación de Sistemas y Telemática gestiona el uso de contraseñas, proporcionando mecanismos contra los ataques de suplantación de identidad y todos aquellos relacionados con el acceso no autorizado a la información. Así mismo, realiza sensibilización al interior del Instituto sobre el uso de contraseñas y la manera segura que éstas deben ser gestionadas, a través de su documento GI-SYT-8 Guía para la Gestión de Contraseñas Seguras.

9.4 Control de Acceso a Sistemas y Aplicaciones

Objetivo: Prevenir el uso no autorizado de sistemas y aplicaciones.

9.4.1 Restricción de acceso a información

Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

- El Instituto cuenta con mecanismos de control de acceso para las áreas seguras (centro de cómputo, centro de cableado y oficinas que almacenen información reservada); tales como: cámaras, puertas de seguridad, sistemas de control con lectores biométricos.
- El Grupo de Sistemas y Telemática tiene asegurada la puerta de acceso al centro de cómputo y centro de cableado, dado que ésta área alberga los servidores que contienen información crítica y debe permanecer cerrada y asegurada y su acceso sólo es permitido a los trabajadores del Grupo de Sistemas y Telemática.
- El Grupo de Sistemas y Telemática cuenta con una bitácora de registro del ingreso de visitantes al centro de cómputo y a los centros de cableado y para acceso a personas externas al grupo sólo se

hace con el acompañamiento de un trabajador del área SYT, la cual se encuentra en un sitio visible para su diligenciamiento.

- Periódicamente se realiza un monitoreo a los ingresos al centro de cómputo y a los centros de cableado para identificar accesos no autorizados y confirmar que los controles de acceso son efectivos.
- Se deben implementar mecanismos de múltiple factor de autenticación para acceso a los sistemas de información del Instituto. Actualmente se tiene acceso de logueo sencillo a los sistemas de información.

9.4.2 Procedimiento de Conexión Segura

Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.

- Toda solicitud de acceso a sistemas y aplicaciones del Instituto deberá hacerse mediante la mesa de servicios: https://invemar.sd.cloud.invgate.net/. Ver también el PR-SYT-4 Procedimiento para la Gestión de Cambios a los Flujos de Laserfiche, Actualizaciones a los Sistemas de Información y Sistemas Operativos.
- Los accesos a los sistemas y aplicaciones institucionales son validados inicialmente a través del directorio activo para ingreso al PC y posteriormente se valida su ingreso en la aplicación específica de acuerdo a los roles y permisos dados a los usuarios para su acceso y teniendo en cuenta las tareas que desarrolla de acuerdo a su cargo.

9.4.3 Sistema de Gestión de Contraseñas

Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.

La Coordinación de Sistemas y Telemática gestiona el uso de contraseñas, proporcionando mecanismos contra los ataques de suplantación de identidad y todos aquellos relacionados con el acceso no autorizado a la información. Así mismo, realiza sensibilización al interior del Instituto sobre el uso de contraseñas y la manera segura que éstas deben ser gestionadas, a través de su documento GI-SYT-8 Guía para la Gestión de Contraseñas Seguras.

- Un usuario registrado y autorizado en el Instituto, se debe autenticar siempre con su contraseña personal para acceder a los sistemas de información y/o a los servicios de la plataforma tecnológica.
- Las contraseñas tendrán un periodo de vigencia de CUARENTA (40) días, fecha en la cual se obligará a cambiarse de acuerdo a las mejores prácticas y lineamientos de seguridad del Instituto, de lo contrario no permite el acceso a la cuenta.
- La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

- Por política de directorio activo, el INVEMAR tiene preestablecido en sus equipos institucionales el bloqueo de cuentas de usuarios luego de realizar cinco (5) intentos fallidos de inicio de sesión.
- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al Grupo de Sistemas y Telemática para que se le proporcione una nueva contraseña.
- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.
- Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.
- Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, deberá cambiarlo inmediatamente.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

9.4.4 Uso de programas utilitarios privilegiados

Control: Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

- Se prohíbe el uso de programas utilitarios, software o aplicaciones no autorizados por parte de los trabajadores sin la debida autorización del Grupo de Sistemas y Telemática.
- El uso de los programas utilitarios privilegiados y de herramientas o utilitarios propios de sistemas operativos está limitado a personal autorizado y su uso está restringido. En caso de ser necesario sólo los trabajadores del Grupo de Sistemas y Telemática está autorizado para hacer uso de éstos, disponiendo de la respectiva trazabilidad de las operaciones realizadas en los casos que han sido autorizados.

9.4.5 Control de Acceso a Códigos Fuente de Programas

Control: Se debe restringir el acceso a códigos fuente de programas.

- El acceso a los códigos fuente de programas y elementos asociados, se debe contar con autorización del Grupo de Sistemas y Telemática y/o del Laboratorio de Sistemas de información, en los casos que la custodia de ésta información este bajo su responsabilidad.

10. CRIPTOGRAFÍA

10.1 Controles Criptográficos

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

10.1.1 Política sobre el uso de controles criptográficos

Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.

- El Grupo de Sistemas y Telemática y el Laboratorio de Sistemas de Información como responsables de la administración de servidores y sistemas de información institucionales, deben establecer roles y responsabilidades para la implementación de una política para la gestión de los mecanismos criptográficos a ser aplicados a las bases de datos que contengan información que deba ser protegida.
- El Grupo de Sistemas y Telemática y el Laboratorio de Sistemas de Información deben establecer una estrategia para cifrar las bases de datos críticas que contengan datos personales, velando por la protección de la confidencialidad, la autenticidad y la integridad de esta información.
- El Grupo de Sistemas y Telemática y el Laboratorio de Sistemas de Información deberá dar a conocer y/o capacitar a los trabajadores en el uso de herramientas de uso criptográfico, cuando se requiera su uso.

10.1.2 Gestión de Claves

Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.

- El Grupo de Sistemas y Telemática y el Laboratorio de Sistemas de Información, apoyados en el documento GI-SYT-8 Guía para la Gestión de Contraseñas Seguras realizará la generación de éstas aplicando procesos de expiración acorde a los criterios establecidos por la herramienta de encriptación y desencriptación y no debe superar 90 días.
- El Grupo de Sistemas y Telemática deberá realizar revisiones periódicas a las herramientas de uso criptográfico (Tokens, Firma Digital, etc.), con el fin de detectar fallas o vulnerabilidades.
- El Grupo de Sistemas y Telemática deberá prestar el debido soporte técnico para la configuración de los usuarios y soluciones adoptadas para controles criptográficos.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

11.1 Áreas Seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

11.1.1 Perímetro de Seguridad Física

Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.

- El Grupo de Sistemas y Telemática cuenta con mecanismos de control de acceso para las áreas seguras (centro de cómputo y centro de cableado); tales como cámaras, sistemas de control con lectores biométricos y llaves.
- Las puertas de acceso al centro de cómputo, el centro de cableado u otras áreas que alberguen información crítica, se mantienen siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentren en las áreas mencionadas permanecen cerrados.
- El centro de cómputo, el centro de cableado y las áreas determinadas como seguras, cuenta con una bitácora de control y registro de ingreso y salida del personal autorizado.

11.1.2 Controles Físicos de Entrada

Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

- El Grupo de Sistemas y Telemática autoriza las solicitudes de acceso al centro de cómputo y áreas consideradas como seguras, administración de infraestructura, centro de cableado y acompaña de manera permanente a los visitantes durante su estancia en estas áreas.
- El Grupo de Sistemas y Telemática tiene implementado un lector biométrico para acceso al centro de cómputo, de manera que las personas que acceden estén debidamente autenticadas a través del lector.
- El Grupo de Sistemas y Telemática realiza acompañamiento al personal de soporte durante su estancia en las áreas seguras.

11.1.3 Seguridad de Oficinas, Salones e Instalaciones

Control: Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.

- El Grupo de Sistemas y Telemática mantiene protegidas las áreas de centro de cómputo y centro de cableado.
- Se debe mantener de manera anónima la confidencialidad de las áreas físicas en donde se custodia la información sensible.

11.1.4 Seguridad de Oficinas, Salones e Instalaciones

Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

- El Instituto cuenta con control de incendios.
- El Instituto cuenta con un plan de emergencias definido por el Grupo de Servicios Generales, con el fin de contar con la protección necesario contra amenazas externas.

11.1.5 Trabajo en áreas seguras

Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.

- El trabajo en áreas seguras no supervisado se debe evitar por razones de seguridad para evitar oportunidades malintencionadas.
- Se deben mantener con llave las áreas seguras vacías y revisar periódicamente.
- Los trabajadores del Instituto, sólo deben conocer la existencia de un área segura

11.1.6 Áreas de Despacho y Carga

Control: Se deben controlar los puntos de acceso tales como áreas de despacho y carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

- El Grupo de Servicios Generales controla la recepción y despacho de la carga.

11.2 Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

11.2.1 Ubicación y protección de los equipos

Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.

- El Instituto tiene los equipos de procesamiento de información (servidores, equipos de comunicaciones) en áreas seguras.
- El Grupo de Sistemas y Telemática, tiene debidamente señalizada las áreas seguras para evitar el consumo de alimentos o bebidas.

- Los sistemas de puesta a tierra están debidamente instalados y protegidos y frecuentemente revisados.

11.2.2 Servicios públicos de soporte

Control: Los equipos se deben estar ubicados proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.

- Los equipos de soporte ambiental y eléctrico instalados, cumplen con los requisitos legales y fueron suministrados e instalados siguiendo las especificaciones de los fabricantes y aplicando la normativa vigente. Se cuenta con la Certificación RETIE para los equipos eléctricos.
- Regularmente se evalúa la capacidad de suministro de energía principal y de soporte, realizando rondas de revisión a la infraestructura eléctrica y se realizan pruebas de funcionamiento a las plantas eléctricas de respaldo.
- Se realiza diariamente rondas de inspección a las condiciones ambientales y eléctricas a las áreas consideradas como seguras tales como: cuartos de UPS, sala de servidores, colección de muestras de museo, cuarto frío de almacenamiento de muestras y cuartos de reactivos. Adicionalmente, se monitorean las temperaturas de estos sitios de forma remota desde un PC.
- Bimestralmente se realiza mantenimiento de todos los aires acondicionados de las áreas críticas y de las redes contraincendios y anualmente se realiza mantenimiento a la subestación eléctrica, plantas de respaldo eléctrico y UPS.

11.2.3 Seguridad del cableado

Control: El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.

- Se cuenta con cableado estructurado debidamente certificado en todos sus puntos de conexión.
- Se cuenta instalado y configurado el sistema eléctrico regulado para la conexión de todos los activos de tecnología.

11.2.4 Mantenimiento de equipos

Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

- El Instituto cuenta con planes de mantenimiento anuales de todos los equipos del Instituto, así como se lleva un monitoreo en la herramienta INVGATE de las características técnicas de los mismos.
- Los planes de mantenimiento son ejecutados en su totalidad de manera satisfactoria y de acuerdo al registro de los mismo en la herramienta INVGATE.

11.2.5 Retiro de activos

Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.

- Los activos del Invemar relacionados con información y software se encuentran debidamente registrados en el documento MT-SYT-1 Matriz de Inventario y Clasificación de Activos de Información por Procesos.
- Los activos del Invemar relacionados con los equipos están debidamente documentados en el documento PR-CTA-10 Procedimiento para el manejo y control administrativo de los activos fijos adquiridos por el Invemar.
- El Grupo de Sistemas y Telemática vela por que la entrada y salida de servidores y demás recursos tecnológicos institucionales de las instalaciones del Instituto, y que esta cuente con la autorización documentada y aprobada previamente.
- El Coordinador de cada área vela porque los equipos que se entren bajo su poder y estén sujetos a traslados físicos fuera del Instituto, posean pólizas de seguro y se informe oportunamente a la Coordinación de Gestión contractual de su movimiento.
- La Coordinación de cada área, previo visto bueno de la Subdirección Administrativa (SRA) es la autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda cualquier trabajador de los recursos tecnológicos del Instituto.
- Para realizar el retiro o salida de los activos fijos del Instituto deberá realizar la solicitud a través de la Intranet Institucional.
- Se debe llevar registro de todos los activos que se retiran del sitio donde están ubicados dejando observaciones respecto de su devolución.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de éstas.

Los trabajadores que retiren activos de las instalaciones del Instituto deberán tener en cuenta:

- Bajo ninguna circunstancia los equipos de cómputo del Instituto pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso de que sea transportado en un vehículo.
- Los equipos portátiles deberán ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes cambios electromagnéticos.
- En caso de pérdida o robo de un equipo, se debe poner la respectiva denuncia ante la autoridad competente e informar de manera inmediata al Coordinador del Grupo de Sistemas y Telemática para tomar las acciones necesarias ante la situación.

11.2.7 Disposición segura o reutilización de equipos

Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o rehúso.

- Cuando un equipo o portátil deba darse de baja, se realizará una copia de seguridad de la información del equipo previamente.
- Cuando un equipo deba ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobre escritura de los medios que contienen información), con el fin de evitar pérdida de información o recuperación no autorizada. Deberá realizar la solicitud al Grupo de Sistemas y Telemática a través de su mesa de servicios (https://invemar.sd.cloud.invgate.net/) registrar la solicitud del proceso de eliminación segura.

11.2.8 Equipos sin supervisión de los usuarios

Control: Los usuarios deben asegurarse de que el equipo no se encuentre sin supervisión y tenga la protección apropiada.

- Cuando un trabajador deba ausentarse de su sitio de trabajo, deberá verificar que la pantalla de su computador este bloqueada, de igual manera, cerrar las aplicaciones que tiene abiertas y habilitadas, evitando que personas ajenas no puedan tener acceso a ésta. Adicionalmente deberá guardar los documentos físicos o digitales que contengan información de uso interno, clasificado o reservado.
- Al realizar impresión de documentos de carácter confidencial (información pública clasificada e información pública reservada), deben ser retirados de la impresora inmediatamente.

11.2.9 Política de escritorio limpio y pantalla limpia

Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia.

- El Instituto tiene establecido el documento DZ-SYT-7 Directriz de Escritorio y Pantalla Limpia, en donde se trazan los lineamientos para prevenir la pérdida, robo o compromiso de la información durante y fuera de las horas laborales en los puestos de trabajo y equipos de cómputo de los trabajadores.
- Los computadores institucionales deben cargar por defecto el fondo de pantalla institucional, el cual se modifica periódicamente y debe permanecer activo en la sesión que se encuentre.
- Se deben cumplir todos los lineamientos contemplados en la directriz.

12. SEGURIDAD DE LAS OPERACIONES

12.1 Procedimientos operacionales y responsabilidades

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

12.1.1 Procedimientos de Operación documentadas

Control: Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.

- El instituto cuenta con los procedimientos operativos requeridos para la adecuada operación y administración del centro de cómputo y el centro de cableado, en dichos procedimientos se contempla las configuraciones y algunas instalaciones de equipos, así como también la recuperación de sistemas, equipos y aplicaciones.
- Los procedimientos operativos se encuentran registrados en el Sistema KAWAK.

12.1.2 Gestión de Cambios

Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

- El Instituto tiene implementado el procedimiento para la gestión de cambios que realiza a los flujos de Laserfiche, a las actualizaciones de los sistemas de información y los sistemas operativos. Ver documento PR-SYT-4 Procedimiento para la Gestión de Cambios a los Flujos de Laserfiche, actualizaciones a los sistemas de información y Sistemas Operativos.

12.1.3 Gestión de Capacidad

Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura para asegurar el desempeño requerido del sistema.

- El Instituto deberá monitorear la capacidad de sus sistemas e infraestructura con la finalidad de garantizar la disponibilidad de sus servicios y proyectar necesidades a futuro que mejoren la prestación de éstos.
- El Instituto realiza el diagnóstico tecnológico anualmente, y consolida la información mediante informe presentado a la Subdirección Administrativa, con la finalidad de tomar las acciones

necesarias que se requieran para mejorar la capacidad presente y futura de la infraestructura tecnológica.

- El Instituto deberá implementar un procedimiento de Gestión de Capacidad, especialmente para los sistemas críticos.

12.1.4 Separación de los ambientes de desarrollo, pruebas y producción

Control: Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.

- El Instituto cuenta con ambientes de desarrollo, prueba y producción para sistemas críticos.
- Para los datos de prueba se cuenta con información debidamente almacenada y protegida.
- Para el acceso a los ambientes se debe cumplir con los requerimientos dados en el documento DZ-SYT-4 Directriz Control de Acceso.

12.2 Protección contra códigos maliciosos

Objetivo: Asegurar de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

12.2.1 Controles contra códigos maliciosos

Control: Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos.

- El instituto proporciona los mecanismos necesarios que garantizan la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por software malicioso.
- Desde la Coordinación de Sistemas y Telemática se proveen herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reducen el riesgo de contagio de software malicioso y respaldan la seguridad de la información contenida y administrada en la plataforma tecnológica del INVEMAR y los servicios que se ejecutan en la misma.
- La Coordinación de Sistemas y Telemática asegura que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

- La Coordinación de Sistemas y Telemática certifica que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- La Coordinación de Sistemas y Telemática, a través de sus trabajadores, se asegura que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- La Coordinación de Sistemas y Telemática, a través de sus trabajadores, certifica que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda https://invemar.sd.cloud.invgate.net/ o al correo soporte@invemar.org.co , para que, a través de ella, la Coordinación de Sistemas y Telemática tome las medidas de control correspondientes.

12.3 Copias de Respaldo

Objetivo: Proteger contra la pérdida de datos.

12.3.1 Copias de respaldo de la información

Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

- El Instituto certifica la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.
- Desde la Coordinación de Sistemas y Telemática se vela por que los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta.
- El sitio externo donde se resguarden las copias de respaldo cuenta con los controles de seguridad física y medioambiental apropiados, acuerdo lo definido en el documento: AX-SYT-9 ANEXO 7. PR-SYT-1 Almacenamiento y Recuperación de copias de seguridad; ubicados en el Sistema Kawak.
- El Instituto a través de la Coordinación de Sistemas y Telemática, establece como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores.

- El Instituto define las condiciones de transporte y custodia de las copias de respaldo de la información que son almacenadas externamente.
- La Coordinación de Sistemas y Telemática proporciona apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos información del Instituto, acuerdo a lo establecido en el documento **DZ-SYT-5** Directriz de Retención de Copias de Seguridad.
- Todos los trabajadores son responsables directos de la generación de los backups o copias de respaldo, asegurándose de validar la copia. Puede solicitar asistencia técnica a través de la mesa de ayuda: https://invemar.sd.cloud.invgate.net/ para la restauración de un backups en caso de requerirlo o apoyarse con el procedimiento **IT-SYT-1** Backup Usuarios Finales y el **PR-SYT-6** Procedimiento Backup Institucional.
- Es responsabilidad de los usuarios de la plataforma tecnológica del INVEMAR identificar la información crítica que debe ser respaldada y almacenada de acuerdo con su nivel de clasificación.

12.4 Registro y Seguimiento

Objetivo: Registrar eventos y generar evidencia.

12.4.1 Registro de Eventos

Control: Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.

- El Instituto debe generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.
- Los logs de auditoría de eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, quedaran registrados de acuerdo con las directrices establecidas por la Coordinación de Sistemas y Telemática.

12.4.2 Protección de la información de registro

Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

- El Instituto debe copiar en tiempo real los logs de registro para evitar pérdida o adulteración de éstos.
- Asignar permisos de acceso a la persona debidamente autorizada para realizar el monitoreo y gestión de riesgos.

- Se debe evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.

12.4.3 Registros del administrador y del operador

Control: Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.

- Para los Logs de los administradores y las cuentas privilegiadas se deben realizar auditorías periódicas para evitar pérdida o adulteración de la información.
- El Instituto debe activar los mecanismos de registro de auditoria en su infraestructura tecnológica que permita realizar el monitoreo de las cuentas y proteger la información.

12.4.4 Sincronización de relojes

Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.

- El Instituto cuenta con un mecanismo de sincronización de relojes para los equipos, servidores, sistemas operativos, sistemas de información y demás elementos de infraestructura utilizados. Igualmente se encuentra alineados con la hora oficial de Colombia desde el sitio web del Instituto Nacional de Metrología.

12.5 Control de software operacional

Objetivo: Asegurarse de la integridad de los sistemas operacionales.

12.5.1 Instalación de software en sistemas operativos

Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

- El INVEMAR, a través de la Coordinación de Sistemas y Telemática, designa responsables y establece el documento DZ-SYT-4 Directriz Control de Acceso y el PR-SYT-4 Procedimiento para la Gestión de Cambios a los Flujos de Laserfiche, Actualizaciones a los Sistemas de Información y Sistemas Operativos, para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

- El software instalado en los PC y servidores del Instituto, se encuentra debidamente licenciado. Para los casos de software libre, está permitido su uso comercial y su instalación debe ser descargada de la página oficial del fabricante.
- El Grupo de Sistemas y Telemática realiza revisiones periódicas del uso del software instalado en los servidores, pc y portátiles del Instituto.
- Cualquier software que viole los derechos de licenciamiento, las directrices y controles de este manual debe ser desinstalado y debe ser reportado el hecho como incidente de seguridad por incumplimiento de la Directriz de seguridad.

12.6 Gestión de vulnerabilidad técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

12.6.1 Gestión de las vulnerabilidades técnicas

Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

- El INVEMAR debe ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y hacking ético.
- Se debe definir planes de cierre de brechas en las vulnerabilidades identificadas donde se identifiquen los responsables de corregir y los plazos para efectuar estas correcciones.
- Se deben definir roles y responsabilidades asociadas con la gestión de vulnerabilidades técnicas, que incluya el seguimiento a la vulnerabilidad, la valoración de riesgos asociados a la vulnerabilidad, la instalación de parches o actualizaciones a los sistemas y su respectivo seguimiento.

12.6.2 Restricciones sobre la instalación de software

Control: Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.

- La instalación de software en lo equipos institucionales debe ser realizada y aprobada por el Grupo de Sistemas y Telemática.
- Los usuarios que utilicen el software instalado en los equipos asignados, deberán cumplir con el principio del mínimo privilegio, es decir, que se le dará los permisos o los accesos a lo que necesita estrictamente para desempeñar sus responsabilidades o funciones laborales.
- Se tienen implementados mecanismos para que los usuarios no realicen instalaciones de software no autorizadas por el Grupo de Sistemas y Telemática.

12.7 Consideraciones sobre auditorías de Sistemas de Información

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

12.7.1 Controles sobre auditorías de Sistemas de Información

Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordad cuidadosamente para minimizar las interrupciones en los procesos de negocio.

- Los requerimientos de auditoría para realizar el acceso a sistemas de información y a datos, se deben acordar con los líderes de procesos y propietarios de sistemas de información, previo a esta revisión.
- El alcance de las pruebas técnicas de auditoría a ser practicado debe ser acordado y controlado.
- Las pruebas técnicas que son aplicadas por la auditoría y que puedan afectar la disponibilidad de los sistemas se deben ejecutar en ventanas de tiempo previamente acordadas y en un ambiente controlado.
- Las pruebas de auditoría sólo tendrán acceso al software y datos en modo lectura.
- Activar mecanismos de auditoría en toda la infraestructura tecnológica que permita registrar las actividades de los administradores, incluyendo evidencia de que estas cuentas no cuentan con privilegios para modificar o eliminar registros de eventos.

13. SEGURIDAD DE LAS TELECOMUNICACIONES

13.1 Gestión de la Seguridad de las Redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte

13.1.1 Controles de redes

Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

- El INVEMAR garantiza que todos sus trabajadores, contratistas y estudiantes, que tengan necesidad de acceder a las redes o recursos de red del Instituto deben seguir los lineamientos de seguridad establecidos en este documento y en la directriz DZ-SYT-4 Directriz Control de Acceso, en el procedimiento PR-SYT-3 Procedimiento para la Administración de Cuentas de Usuario,

contribuyendo a preservar la confidencialidad, integridad y disponibilidad de la información del Instituto.

- El Grupo de Sistemas y Telemática como responsable de las redes de datos y de los recursos de red del instituto, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.
- El Grupo de Sistemas y Telemática asegurará que las redes inalámbricas del instituto cuenten con métodos de autenticación que evite accesos no autorizados.
- El Coordinador del Grupo Sistemas y Telemática, con el apoyo del Jefe de Telemática y Hardware, establecerá controles para la identificación y autenticación de los usuarios proveedores o externos, en las redes o recursos de red del Instituto, así como velará por la aceptación de las responsabilidades de dichos terceros.
- Los usuarios de las áreas del INVEMAR no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del Instituto, sin la autorización del Coordinador del Grupo de Sistemas y Telemática.
- Todos los computadores de usuario final, que se conecten o deseen conectarse, a las redes de datos del Instituto, deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- El Grupo de Sistemas y Telemática debe establecer controles, para la identificación y autenticación de los usuarios, provistos por proveedores y terceros, en las redes o recursos de red del Instituto, así como velar por la aceptación de las responsabilidades de dichos proveedores y terceros.
- El Coordinador del Grupo de Sistemas y Telemática autoriza la creación, modificación o eliminación de las cuentas de acceso a las redes o recursos de red del Instituto.
- La Coordinación del Grupo de Sistemas y Telemática debe promover la confidencialidad, integridad y disponibilidad a través de las redes y sus segmentos tanto en las redes públicas con en las inalámbricas.

13.1.2 Seguridad de los servicios de red

Control: Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

- El Grupo de Sistemas y Telemática garantiza que los servicios de red son monitoreados con regularidad, garantizando la disponibilidad de los sistemas de información.

- En los acuerdos de nivel de servicio se identifican los niveles de requisitos de seguridad necesarios para los servicios contratados.

13.1.3 Separación en las redes

Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.

- El Grupo de Sistemas y Telemática garantiza la separación de las redes lógicas de los diferentes servicios de TI.
- El INVEMAR tiene definidos los mecanismos de autenticación y protocolos de seguridad para el acceso a redes.

13.2 Transferencia de Información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

13.2.1 Políticas y procedimientos de transferencia de información

Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de la información, mediante el uso de todo tipo de instalaciones de comunicaciones.

- El INVEMAR a través de la Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de Información, asegurarán la protección de la información en el momento de ser transferida o intercambiada con otras entidades, y establecerá los procedimientos y controles necesarios para el intercambio de información. Para tal efecto, se tiene documentado el PR-LABSIS-3 Entrega en Custodia al LABSIS de Objetos Digitales producto de las actividades misionales del INVEMAR.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de Información debe definir y establecer un mecanismo para realizar el intercambio de información con los diferentes terceros que, hacen parte de la operación del INVEMAR, recibiendo o enviando información del instituto y que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.

- Los propietarios de los activos de información deben velar porque la información del INVEMAR o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

- Los propietarios de los activos de información deben propender por que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

- El INVEMAR tiene dispuesto en los contratos de trabajo y las minutas de contratación con terceros una cláusula de confidencialidad, sobre el uso y acceso a la información institucional donde

13.2.2 Acuerdos sobre transferencia de información

Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de Información debe autorizar el establecimiento del vínculo de transmisión de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.
- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

- Los propietarios de los activos de información con el acompañamiento de la Coordinación de Sistemas y Telemática y del Laboratorio de Servicios de Información deben asegurarse que el intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a los Lineamientos de seguridad de control de acceso a redes y recursos de red y de privacidad y protección de datos personales del INVEMAR definidos en el documento DZ-SYT-7 Directriz Control de Acceso.

- Los propietarios de los activos de información deben verificar la destrucción de la información suministrada una vez se ha cumplido el cometido por el cual fue enviada y en caso de ser necesario.

- La Oficina de Archivo y Correspondencia debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por el INVEMAR, y que estos permitan ejecutar rastreo de las entregas.

13.2.3 Mensajería Electrónica

Control: Se deben proteger apropiadamente la información incluida en los mensajes electrónicos.

- El INVEMAR garantiza la disponibilidad del correo electrónico institucional constituyéndolo como una poderosa herramienta de trabajo, que permite la transferencia de información, no sólo dentro del Instituto, sino también externamente, en forma eficiente y ágil; y cualquier uso indebido del mismo puede afectar severamente la imagen y la reputación del Instituto. Para este lineamiento

se establece como referencia lo contenido en el documento MN-SYT-10 Manual de Lineamientos de uso de internet, correo y chat institucional.

- La Coordinación de Sistemas y Telemática provee un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.

- La Coordinación de Sistemas y Telemática establece procedimientos e implanta controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

- La Coordinación de Sistemas y Telemática genera campañas para concientizar tanto a los trabajadores internos, como al personal provisto por terceras partes y prestación de servicios, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

- Cada trabajador que tenga una cuenta de correo asignada es un usuario del sistema y es responsable de los recursos que tenga asignados y de todas las acciones que se lleven a cabo en su utilización.

- Los usuarios del correo electrónico institucional son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

- Los servicios de correo electrónico Institucional se emplean para servir a una finalidad operativa y administrativa en relación con el cargo que desempeña. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura tecnológica del INVEMAR se consideran bajo el control del Instituto.

- El correo electrónico debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el INVEMAR y no debe utilizarse para ningún otro fin.

- El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.

- No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre del Instituto.

- Cuando un trabajador, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire del INVEMAR, su cuenta de correo será desactivada.

- El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en el INVEMAR.

- Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por el INVEMAR.

- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte del Instituto.

- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta soporte@invemar.org.co con la frase "correo sospechoso" en el asunto.

- El único servicio de correo electrónico autorizado en el Instituto es el asignado por el Grupo de Sistemas y Telemática.

- En general, el uso del correo electrónico institucional está restringido a asuntos laborales, su empleo para asuntos personales corresponde a cada usuario velar por que la gestión de la información contenida en su correo electrónico sea la más adecuada. Para ello, debemos revisar periódicamente la bandeja de entrada y, si procede, la de salida, como mínimo una vez al día.

- Está prohibido utilizar el sistema de correo electrónico institucional para el desarrollo de actividades políticas, comerciales o de entretenimiento o para la transmisión de mensajes vulgares u obscenos.

- Todos los usuarios que posean acceso autorizado al correo electrónico, deberán mantener un adecuado, ético y responsable uso de este recurso, cuidando no dañar la imagen y reputación del Instituto ni de ninguno de sus usuarios.

- Los mensajes que formen parte de un procedimiento, u otros que deban conservarse, tienen que estar debidamente archivados en la carpeta correspondiente, puesto que es previsible que se borren al cabo de un tiempo o se llegue a un tope de capacidad. Los correos electrónicos con fines privados deben ser borrados o movidos cada día por si es necesario hacer un traspaso o eliminación de la cuenta por motivos técnicos.

13.2.4 Acuerdo de confidencialidad o de no divulgación

Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

- El INVEMAR garantiza que los trabajadores, contratistas y terceros, firmen como parte de los términos y condiciones iniciales de trabajo, el acuerdo de confidencialidad, el cual está incluido en una cláusula dentro del contrato laboral, así como para contratos de prestación de servicios o contractuales.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1 Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.

14.1.1 Análisis y especificación de requisitos de seguridad de la información

Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

- El INVEMAR asegura que el software adquirido y desarrollado, cumple con los controles y requisitos de seguridad y calidad. Para el caso de desarrollos propios, el Instituto, debe verificar que están completamente documentados, que las diferentes versiones se preservan adecuadamente en varios medios y se guarda copia de respaldo externa al Instituto.

- Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica del INVEMAR, por cualquier dependencia o proyecto, deberá ser gestionado por la Coordinación de Sistemas y Telemática para su correcto funcionamiento.

- La Coordinación de Sistemas y Telemática y su equipo de trabajo, será la única dependencia autorizada para realizar copia de seguridad del software original.

- La instalación del software en los equipos de cómputo del INVEMAR, se realizará únicamente a través de solicitud a la Mesa de Ayuda https://invemar.sd.cloud.invgate.net/

- El software proporcionado por el INVEMAR no puede ser copiado o suministrado a terceros.

- En los equipos del Instituto se podrá sólo utilizar el software licenciado y autorizado por la Coordinación de Sistemas y Telemática.

- Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Coordinación de Sistemas y Telemática con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.

- El software que se adquiera a través de los proyectos o programas debe quedar a nombre del INVEMAR.

14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

Control: La información involucrada en servicios de aplicaciones que pasan sobre redes públicas, se debe proteger de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas.

- El Grupo de Sistemas y Telemática cuenta con un sistema de administración de contenidos del portal web que le permiten realizar la publicación de la información por parte de los encargados.
- Las aplicaciones que se administran a través de redes públicas, cuentan con mecanismos de protección de información.

14.1.3 Protección de transacciones de servicios de aplicaciones

Control: La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.

- Las dependencias propietarias de los sistemas de información, en acompañamiento con la Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de Información, establece las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

- La Coordinación de Sistemas y Telemática y la Jefatura de Laboratorio de Servicios de Información, lideran la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.
- El INVEMAR cuenta con usuarios y claves de acceso a las cuentas bancarias, adicionalmente para la realización de pagos, el método de autenticación se realiza a través de token y firmas digitales.

- Se tiene establecido el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

14.2 Seguridad en los procesos de desarrollo y soporte

Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

14.2.1 Política de desarrollo seguro

Control: Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.

- El INVEMAR garantiza que el desarrollo interno o externo de los sistemas de información cumplan con los requerimientos de seguridad, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.

- Los desarrolladores realizan las pruebas al software desarrollado y registran en las plataformas BitBucket y Jira los eventos de creación de código en línea y control de versión de los códigos creados e integran sin problemas las incidencias con el código fuente para poder realizar un seguimiento de principio a fin.

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de información implanten los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de Información deben contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del INVEMAR, para este caso se implementó la plataforma BitBucket para realizar este control.
- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de información, con el apoyo de sus equipos de trabajo, deben asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información sean estables para realizar sus respectivas pruebas de funcionalidad.

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que presente el software aplicativo del Instituto; dicho soporte debe contemplar tiempos de respuesta aceptables.

- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

14.2.2 Procedimiento de Control de Cambios en Sistemas

Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo de se deberían controlar mediante el uso de procedimientos formales de control de cambios.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de información, con el apoyo de sus equipos de trabajo, son los responsables de planificar, desarrollar y ejecutar las actividades relacionadas con los desarrollos, actualizaciones e instalaciones de software. Adicionalmente, debe planificar la ejecución de pruebas funcionales y de seguridad de sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.
- Al realizar la ejecución de control de cambios se tendrá en cuenta lo establecido en el documento PR-SYT-4 Procedimiento para la Gestión de Cambios a los Flujos de Laserfiche, actualizaciones a los sistemas de información y sistemas operativos.

14.2.3 Revisión técnica de las aplicaciones después de efectuar cambios en sistema operativo

Control: Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de información, realizan verificación frecuente de los cambios en los servidores y en las aplicaciones, respecto al impacto que puedan tener éstos dando cumplimiento a los lineamientos de seguridad de la información.

14.2.4 Restricciones sobre los cambios de paquetes de software

Control: Se deben evitar las modificaciones a los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.

- El INVEMAR sólo utiliza software licenciado y adquirido a través de un proveedor autorizado. Las actualizaciones de aplicaciones y parches son suministrados por el proveedor y son aplicados estrictamente con las indicaciones que éstos entreguen.
- El INVEMAR no realiza cambios sobre los paquetes de software adquiridos.

14.2.5 Principios de construcción de sistemas seguros

Control: Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.

- El INVEMAR debe documentar, aplicar y exigir que la construcción de sistemas de información este soportada con requerimientos de diseño de arquitectura segura, que incluya capas de negocio, datos, aplicaciones y tecnología; y deben actualizarse con regularidad para combatir nuevas amenazas potenciales.
- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que presente el software aplicativo del Instituto; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

14.2.6 Ambiente de Desarrollo seguro

Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

- El INVEMAR velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.

- Los desarrolladores realizarán las pruebas al software desarrollado y registrará en las plataformas BitBucket y Jira para los eventos de creación de código en línea y control de versión de los códigos creados e integrar sin problemas las incidencias con el código fuente para poder realizar un seguimiento de principio a fin.

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de información implantan los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de información deben contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del INVEMAR, para este caso se implementó la plataforma BitBucket para realizar este control.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de información se aseguran que los sistemas de información adquiridos o desarrollados a la medida cuenten con licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de información, con el apoyo de sus equipos de trabajo, deben asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información sean estables para realizar sus respectivas pruebas de funcionalidad.

14.2.7 Desarrollo contratado externamente

Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.

- Para los desarrollos de aplicaciones por parte de un proveedor externo se deben aplicar las directrices y lineamientos de seguridad de la información establecidas por el INVEMAR, así como,

las buenas prácticas en los procesos de desarrollo, que incluyan compromisos de confidencialidad, derechos de propiedad intelectual y condiciones de soporte y mantenimiento.

- La Coordinación de Sistemas y Telemática debe certificar que todo el software que se ejecuta en el INVEMAR esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución.

14.2.8 Pruebas de seguridad de sistemas

Control: Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.

- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

- Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

14.2.9 Pruebas de aceptación de sistemas

Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.

- Los desarrolladores realizan las pruebas de aceptación junto con el usuario que hace el requerimiento, de manera que lo desarrollado cumpla con lo esperado. El usuario que realiza el requerimiento es quien aprueba el producto.
- Las pruebas se realizan en un ambiente de pruebas, donde la información contenida en las bases de datos son una réplica exacta de la información de las bases de datos en producción, asegurando que el producto no introducirá vulnerabilidades al ambiente de producción.

14.3 Datos de Prueba

Objetivo: Asegurar la protección de los datos usados para pruebas.

14.3.1 Protección de Datos de Prueba

Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.

- Para los datos de prueba se aplican los procedimientos de control de acceso que se tienen en los ambientes de producción los datos.
- Para los datos de prueba no se utiliza información de datos personales o confidenciales.
- Los datos de prueba se mantienen en los ambientes de prueba para ser reutilizados de ser necesario.
- La Coordinación de Sistemas y Telemática y el Laboratorio de Servicios de Información aseguran que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.

15. RELACIONES CON LOS PROVEEDORES

15.1 Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

15.1.1 Directriz de seguridad de la información para las relaciones con proveedores

Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.

- El INVEMAR establece mecanismos de control en sus relaciones con sus proveedores o terceros, con el objetivo de asegurar que la información o servicio a la que tengan acceso cumplan con los lineamientos, normas y procedimientos de seguridad de la información.
- Los trabajadores responsables de la realización y/o firma de contratos o convenio con proveedores o terceros, se asegurarán de informar sobre lineamientos, normas y procedimientos de seguridad de la información que les apliquen.
- En coordinación con el Grupo de Gestión Contractual, la Coordinación de Sistemas y Telemática implementará en sus contratos con proveedores o terceros, los Acuerdos de Niveles de Servicio (ANS) y los requisitos de seguridad de la información que deben cumplir, así mismo, deberá divulgar a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos, que incluyan estos requisitos.
- El Grupo de Gestión Contractual, en sus contratos con proveedores o terceros, establece cláusulas de confidencialidad y acuerdos de intercambio de información en caso de requerirse.
- La Coordinación de Sistemas y Telemática establece las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red da datos del INVEMAR.

15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

- Los supervisores de los contratos deben asegurar que se comuniquen las directrices, lineamientos y procedimientos de seguridad de la información a los proveedores y contratistas.
- Los supervisores de los contratos deben administrar los cambios en el suministro de servicios contratados manteniendo los niveles de cumplimiento de servicio, seguridad de la información establecidos con ellos y monitoreando la aparición de nuevos riesgos.
- Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal al Coordinador del Grupo de Sistemas y Telemática.
- Desde la Coordinación de Sistemas y Telemática se establece las condiciones de comunicación segura y la transmisión de información desde y hacia los terceros proveedores de servicios.

15.1.3 Cadena de suministro de tecnología de información y comunicación

Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

- Los supervisores de los contratos con proveedores o terceros, administran los cambios en la cadena de suministro de servicios y productos por parte de los proveedores, manteniendo los niveles de cumplimiento del servicio, así como las prácticas de seguridad establecida con ellos y monitoreando la aparición de nuevos riesgos.
- Los supervisores de los contratos deberán validar el cumplimiento de los servicios y productos contratados que estén de acuerdo con los requisitos de seguridad definidos.

15.2 Seguridad de la información en las relaciones con los proveedores

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

15.2.1 Seguimiento y revisión de los servicios de los proveedores

Control: Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

- Los supervisores de los contratos con proveedores o terceros realizan seguimiento al servicio o producto, evaluando el desempeño de los proveedores con base en los acuerdos de nivel de servicios establecidos para validar los niveles de seguridad de la información acordados.

- Desde el Grupo de Sistemas y Telemática se tiene control sobre todos los aspectos de seguridad de la información para las instalaciones de procesamiento de información a las que se tiene acceso, procesa o gestiona un proveedor.

15.2.2 Gestión de cambios a los servicios de los proveedores

Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.

- En los servicios establecidos con los proveedores se deben gestionar todos los cambios siguiendo los procedimientos definidos por el INVEMAR, teniendo en cuenta los cambios en los acuerdos con el proveedor y los cambios requeridos por el Instituto.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 Gestión de incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades

16.1.1 Responsabilidades y procedimientos

Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- La gestión de incidentes de seguridad debe estar basada en los lineamientos del documento PR-SYT-7 Procedimiento de Gestión de Incidentes de Seguridad de la Información, donde se establece el alcance, responsables y el procedimiento a seguir para reportar un incidente de seguridad de la información.
- La Coordinación de Sistemas y Telemática asegura la existencia de documentación de los procedimientos detallados para restaurar equipo, aplicativos, sistemas operativos, bases de datos, archivos de información, entre otros.
- La Coordinación de Sistemas y Telemática con el apoyo de su equipo de trabajo debe realizar los análisis de impacto al negocio (BIA-Bussiness Impact Analysis) y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse al Plan de Contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

16.1.2 Informe de eventos de seguridad de la información

Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.

- El INVEMAR proporcionará los recursos suficientes para dar una respuesta pronta, efectiva y ordenada a los incidentes de seguridad o eventos catastróficos que se presente y que afecten la continuidad de su operación. Así mismo, mantendrá canales de comunicación adecuados hacia trabajadores, proveedores y terceras partes interesadas.
- Al presentarse un evento de seguridad de la información deberá seguir el procedimiento PR-SYT-7 Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- La Dirección General o a quien el Director delegue, es el único autorizado para reportar incidentes de seguridad ante las autoridades; así mismo, es el único canal de comunicación autorizado para hacer pronunciamientos oficiales ante entidades externas.

16.1.3 Informe de debilidades de seguridad de la información

Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

- Todos los trabajadores, contratistas o terceros deberán reportar a través de los canales definidos en el PR-SYT-7 Procedimiento de Gestión de Incidentes de Seguridad de la Información, cualquier situación que se pueda considerar como una debilidad en la seguridad de la información institucional.
- Los lineamientos de gestión y tratamiento de incidentes de seguridad de la información, será aplicada por la Coordinación de Sistemas y Telemática.
    - Los propietarios o custodios de la información, deben informar a la Coordinación de Sistemas y Telemática y/o al Jefe de Telemática y hardware a través de la mesa de servicios https://invemar.sd.cloud.invgate.net/ dispuesta para ello, los incidentes de seguridad de la información identificados y reportados.

16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

- La Coordinación de Sistemas y Telemática evalúa todos los incidentes de seguridad identificados y reportados, de acuerdo a sus circunstancias particulares e informa al Jefe de Telemática y Hardware sobre el tema.
- La Coordinación de Sistemas y Telemática designa personal calificado, para investigar adecuadamente, los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su aparición nuevamente.

16.1.5 Respuesta a Incidentes de seguridad de la información

Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

- La Coordinación de Sistemas y Telemática creará bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento. Estas bases se encuentran configuradas en la herramienta de la mesa de servicio.
- Se debe gestionar adecuadamente los incidentes de seguridad de la información identificados con base en el documento PR-SYT-7 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

- Se debe documentar todo el manejo y gestión de incidentes de seguridad a través de la mesa de servicios, de manera que la base de conocimiento sea alimentada con cada caso presentado y gestionar con ello las lecciones aprendidas y fortaleciendo controles y lineamientos.

16.1.7 Recolección de evidencia

Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

- Se deben definir mecanismos para la recolección de evidencias, así como también contar con una Guía para el levantamiento de evidencias por parte del Grupo de Sistemas y Telemática.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

17.1 Continuidad de Seguridad de la Información

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

17.1.1 Planificación de la continuidad de la seguridad de la información

Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante crisis o desastres.

- La Coordinación de Sistemas y Telemática, lidera los temas relacionados con la continuidad del negocio y la recuperación ante desastres.
- Las Coordinaciones de Sistemas y Telemática y Servicios Generales, deben reconocer las situaciones que serán identificadas como emergencia o desastre para el Instituto, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- La Coordinaciones de Sistemas y Telemática con el apoyo de su equipo de trabajo debe realizar los análisis de impacto al negocio (BIA-Bussiness Impact Analysis) y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de

activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

17.1.2 Implementación de la continuidad de la seguridad de la información

Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

- La Coordinación de Sistemas y Telemática en conjunto con su equipo de trabajo, elabora un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
- La Coordinación de Sistemas y Telemática debe definir directrices y controles de seguridad de la información aplicables ante situaciones adversas.
- La Coordinación de Sistemas y Telemática deberá contemplar un sitio alterno, donde los controles implementados de producción deben ser consistentes y estables con el sitio alterno.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

- La Coordinación de Sistemas y Telemática, con el apoyo de su equipo de trabajo, deben asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.
- Cualquier cambio de seguridad aplicado en el ambiente de producción deberá ser aplicado de la misma manera en el ambiente de contingencia y ser documentado.
- Se deberá implementar un Plan de Recuperación de Desastres (DRP) para el Instituto.

17.2 Redundancia

Objetivo: Asegurarse de la disponibilidad de instalaciones de procesamiento de información.

17.2.1 Disponibilidad de instalaciones de procesamiento de información

Control: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

- El INVEMAR deberá establecer una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para el Instituto.
- La Coordinación de Sistemas y Telemática analizará y establecerá los requerimientos de redundancia para los sistemas de información críticos para el Instituto y la plataforma tecnológica que los apoya.
- La Coordinación de Sistemas y Telemática evaluará y aprobará soluciones de redundancia tecnológica y seleccionar la mejor opción que cumpla con los requerimientos del Instituto.
- La Coordinación de Sistemas y Telemática, a través de sus trabajadores, administrará las soluciones de redundancia tecnológica y realizará pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad del Instituto.
- Se debe implementar redundancias en el Plan de Recuperación de Desastres (DRP) con el fin de garantizar el funcionamiento de las redundancias establecidas.
- Se debe identificar los riesgos asociados a las redundancias establecidas.

18. CUMPLIMIENTO

18.1 Cumplimiento de Requisitos de Ley y Contractuales

Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

18.1.1 Identificación de los requisitos de legislación y contractuales aplicables

Control: Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes y el enfoque de la organización para cada sistema de información y para la organización.

- El INVEMAR velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.
- El INVEMAR cuenta con normograma, donde se establecen los requisitos de las partes interesadas aplicables a seguridad de la información.
- Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los trabajadores, contratistas y personal por prestación de servicios. En caso de que se violen los lineamientos de seguridad ya sea de forma intencional o por negligencia, el Instituto tomará las acciones disciplinarias y legales correspondientes.

18.1.2 Derechos de Propiedad Intelectual

Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.

- La Coordinación de Sistemas y Telemática certifica que todo el software que se ejecuta en el Instituto está protegido por derechos de autor y cuenta con licencia de uso, así como también cuenta con software de libre distribución y uso.

- La Coordinación de Sistemas y Telemática establecer un inventario con el software y sistemas de información que se encuentran permitidos en los computadores y equipos portátiles a través de la herramienta INVGATE, para el desarrollo de las actividades laborales, así como verifica periódicamente que el software instalado en dichos equipos corresponda únicamente al permitido.

- Es ilegal duplicar software o su documentación sin la debida autorización de la Coordinación de Sistemas y Telemática, su reproducción no autorizada es una violación de Ley.

- El Grupo de Gestión Contractual incluye cláusulas de propiedad intelectual y derechos de autor en contratos, que protegen el software, documentos, derechos de diseño, marcas registradas, patentes y códigos fuente.

18.1.3 Protección de registros

Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

- La Coordinación de Sistemas y Telemática está obligado a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos legales o regulatorios contra la pérdida de confidencialidad, integridad y disponibilidad, siguiendo las directrices del documento GI-SYT-3 Guía para la elaboración del inventario y la clasificación de los activos de información.
- El INVEMAR implementa mecanismos de protección de registros de registros tales como bases de datos, transacciones de auditoría, registros de operación definiendo el periodo de retención y medios de almacenamiento (físico o digital), considerando las recomendaciones de los fabricantes para evitar la posibilidad de deterioro.

18.1.4 Privacidad y protección de información de datos personales

Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando se aplicable.

- El INVEMAR cuenta con el documento GI-JUR-1 Guía de Tratamiento de Datos Personales, donde se definen las directrices para su tratamiento.
- El INVEMAR garantiza que los datos personales almacenados, en los sistemas de información, repositorios y recursos informáticos del Instituto, reciban una protección óptima para preservar la confidencialidad, integridad y disponibilidad, en cumplimiento de la Ley 1581 de 2012.
- El INVEMAR protege la privacidad de la información personal de sus trabajadores, estableciendo los controles necesarios para preservar aquella información que el Instituto conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del Instituto y no sea publicada, revelada o entregada a trabajadores o terceras partes sin autorización.
- Las áreas que procesan datos personales de beneficiarios, trabajadores, proveedores y personal por prestación de servicios deben asegurar que sólo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

18.1.5 Reglamentación de controles criptográficos

Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.

- El INVEMAR se regirá por la Ley 527 de 1999 (Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación) y sus decretos reglamentarios, según aplique.

18.2 Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

18.2.1 Revisión independiente de la seguridad de la información

Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

- El INVEMAR realiza proceso de evaluación, control y mejora a través de auditorías internas de revisión anualmente. Esta revisión asegura la conveniencia, la adecuación y la eficacia continua para gestionar la seguridad de la información. Esta revisión es realizada por la Oficina de Control Interno e incluye valoración de las oportunidades de mejora y la necesidad de efectuar cambio en el enfoque hacia la seguridad acuerdo a lo establecido en el Modelo de Seguridad y Privacidad de la Información de MINTIC –MSPI-.

18.2.2 Cumplimiento con las políticas y normas de seguridad

Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.

- El Grupo de Sistemas y Telemática realiza de manera periódica (anualmente) de los sistemas de información para determinar el cumplimiento de las directrices y procedimientos de seguridad de la información.
- El Grupo de Sistemas y Telemática deberá realizar la revisión de los resultados de evaluación de las directrices y procedimientos de seguridad e implementar acciones correctivas sobre las no conformidades identificadas.

18.2.3 Revisión del cumplimiento técnico

Control: Los sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.

- El Grupo de Sistemas y Telemática deberá realizar pruebas técnicas (penetración, análisis de vulnerabilidades, hacking ético, ente otros), para validar el cumplimiento de las directrices, procedimientos y controles de seguridad de la información.

5. TÉRMINOS Y DEFINICIONES

Decreto 2573 de 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de. Acceso a la Información Pública Nacional.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Modelo de Seguridad y Privacidad de la información – MINTIC. Lineamientos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL.

Norma. NTC-ISO-IEC 27001. Sistemas de Gestión de la Seguridad de la Información – Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Resolución 500 de 2021. Por el cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.

Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Resolución 746 de 2022. Por el cual se fortalece el Modelo de Seguridad y Privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.

6. DOCUMENTOS RELACIONADOS

DZ-SYT-1 Directriz de Privacidad, Uso y Derechos de Autor del Portal.

DZ-SYT-2 Directriz General de Seguridad y Privacidad de la Información.

DZ-SYT-4 Directriz Control de Acceso.

DZ-SYT-5 Directriz de Retención de Copias de Seguridad.

DZ-SYT-6 Directriz para Uso de Dispositivos Móviles.

MN-SYT-5 Manual de Usuario Intranet INVEMAR.

MN-SYT-6 Guía Gestor Electrónico Documental (GED) Usuario Final.

MN-SYT-9 Manual De Usuario: Solicitud De Propuestas De Investigación En Laserfiche

MN-SYT-10 Manual de Lineamientos de Uso de Internet, Correo y Chat Institucional.

MT-SYT-1 Matriz de Inventario y Clasificación de Activos de Información por Procesos.

MT-SYT-2 Catálogo de Sistemas de Información.

MT-SYT-4 Catálogo de Sistemas de Información.

GI-JUR-1 Guía de Tratamiento de Datos Personales.

GI-SYT-2 Buenas Prácticas en el Respaldo de la Información.

GI-SYT-3 Guía para la Elaboración del Inventario y la Clasificación de Activos de Información.

GI-LABSIS-5 Metodología para la Administración de Proyectos de Software INVEMAR.

GI-SYT-8 Guía para la Gestión de Contraseñas Seguras.

PL-SYT-3 Plan Estratégico de Seguridad y Privacidad de la Información.

PL-SYT-4 Plan de Capacitación, Sensibilización y Comunicación en Seguridad de la Información.

PL-SYT-5 Plan de Control Operacional de la Seguridad de la Información del INVEMAR.

PR-LABSIS-1 Procedimientos para Identificar e Implementar Actualizaciones de Software para Bases de Datos y Aplicaciones de Terceros.

PR-LABSIS-3 Entrega en Custodia a LABSIS de Objetos Digitales producto de las actividades misionales del INVEMAR.

PR-SYT-1 Procedimiento de Contingencias de Servicios Informáticos.

PR-SYT-2 Procedimiento para Mantenimientos Preventivos.

PR-SYT-3 Procedimiento para la Administración de Cuentas de Usuario.

PR-SYT-4 Procedimiento para la Gestión de Cambios a los Flujos de Laserfiche, actualizaciones a los sistemas de Información y Sistemas Operativos.

PR-SYT-5 Procedimiento para reversar cambios y recuperar archivos de OneDrive.

PR-SYT-6 Procedimiento Backup Institucional.

PT-SYT-1 Protocolo de ingreso al Centro de Datos.

RG-TAL-1 Reglamento Interno de Trabajo.

IT-SYT-1 Backup Usuarios Finales.

IT-SYT-2 Instructivo de Mesa de Ayuda SYT

IT-SYT-3 Instructivo para Diligenciar Hojas de Vida de Servidores.

IT-LABSIS-6 Instructivo de Registro, Revisión e Instalación para las Bases De Datos y Aplicaciones de Terceros.

OT-SYT-1 Catálogo de Servicios Tecnológicos.

FT-SYT-6 Lista de Chequeo de Recepción y entrega de Equipos de Cómputo.

AX-SYT-1 ANEXO 1. PR-SYT-1 Directorio de empleados críticos para el servicio.

AX-SYT-2 ANEXO 2. PR-SYT-1 Recuperación Oracle.

AX-SYT-3 ANEXO 3. PR-SYT-1 Recuperación del Servidor Firewall.

AX-SYT-7 ANEXO 5. PR-SYT-1 Recuperación de Conectividad.

AX-SYT-8 ANEXO 6. PR-SYT-1 Recuperación Servidor de Aplicaciones Tayrona.

AX-SYT-9 ANEXO 7. PR-SYT-1 Almacenamiento y Recuperación de Copias de Seguridad.

AX-SYT-10 ANEXO 8. PR-SYT-1 Directorio de Proveedores Críticos para el Servicio.

AX-SYT-11 ANEXO 9. PR-SYT-1 Inventarios de Sistemas y Equipos Críticos.

AX-SYT-12 ANEXO 1. DZ-SYT-2 Roles y Cargos Equipo de Gestión de Seguridad y Privacidad de la Información y Plan Estratégico de Tecnologías de la Información PETI.

Elaborado por:	Cargo:
Edith Constanza Soler D.	Auxiliar Sistemas y Telemática
Revisado por: Raúl N. Carrerá V. Benjamín Lobato Janer Pontones	Cargo: Coordinador Sistemas y Telemática Jefe de Telemática y Hardware Jefe de Proyectos de Software

Revisado por: Sandra Rincón Cabal	Cargo: Subdirector Administrativa
Aprobado por: Francisco Arias Isaza	Cargo: Director General INVEMAR
Fecha de implementación: (Aplica para copias en PDF y físicas).	2024-12-13

7. CONTROL DE CAMBIOS DEL DOCUMENTO

VERSIÓN	Fecha	CAMBIO REALIZADO	Responsable
1.0	05/04/2018	Documento Inicial	Constanza Soler
2.0	06/07/2020	Actualización de Documento	Constanza Soler
3.0	01/09/2022	Actualización de documento	Constanza Soler
4.0	20/10/2023	Actualización de documento	Constanza Soler
5.0	13/12/2024	Actualización documento	Constanza Soler