1. OBJETIVO

Establecer los lineamientos generales para definir las actividades de seguridad de la información, las cuales se encuentran asociadas a los roles que interactúan con el Instituto de Hidrologia, Meteorología y Estudios Ambientales IDEAM.

2. ALCANCE

Este manual dependerá de los roles y las responsabilidades de la seguridad de la información y las metas establecidas, permitiendo la diferenciación de las actividades propias de cada proceso, por otro lado, elegir fácil y adecuadamente un responsable garantizando la asignación y desarrollo de actividades propias de cada Rol.

3. NORMATIVIDAD

Ver Nomograma

4. DEFINICIONES

- **Acción correctiva:** Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

- **Aceptación del riesgo**: Decisión informada de asumir un riesgo concreto.

- **Activo de información:** Cualquier elemento físico, tecnológico tangible o intangible que genera, almacena o procesa información y tiene valor para la organización. La información, como activo corporativo, puede existir de muchas formas:
  - Impresa
  - Almacenada electrónicamente
  - Trasmitida por medios electrónicos
  - Mostrada en videos
  - Suministrada en una conversación
  - Conocimiento de las personas

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Auditor:** Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

- **Autenticación:** Provisión de una garantía de que una característica afirmada por una entidad es correcta.

- **Autenticidad:** Propiedad de que una entidad es lo que afirma ser.

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Declaración de aplicabilidad:** (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

- **Denial of Service (DoS) – Denegación de Servicios:**[1] Limitación o interrupción de acceso autorizado a un recurso del sistema o la demora en las operaciones y funciones del sistema.

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

- **Evento de seguridad de la información:** La ocurrencia detectada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad

- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Gestión de riesgos: A**ctividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- **Identificación de riesgos:** Proceso de encontrar, reconocer y describir riesgos.

- **Impacto:** El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.-.

- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

- **Inventario de activos: L**ista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **Malware o Código Malicioso:** Programas o código escrito con el fin de obtener información acerca de sistemas y usuarios, destruir datos de un sistema, proveer un punto de apoyo para una mayor intrusión a un sistema, falsificar datos y reportes de un sistema, o provocar consumo de tiempo para irritar el funcionamiento de un sistema y al personal de mantenimiento.

- **No conformidad:** Incumplimiento de un requisito.

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgo residual:** El riesgo que permanece tras el tratamiento del riesgo.

- **Seguridad:**
  - Medidas adoptadas para proteger un sistema.
  - Condición de un sistema que resulta del establecimiento y mantenimiento de medidas para proteger el sistema.
  - Estado de los recursos de un sistema libres de acceso no autorizado y de cambios, destrucción o pérdidas accidentales o no autorizados.
  - Capacidad de un sistema basado en computador para proveer la confianza adecuada de que personas y sistemas no autorizados no pueden ni modificar software y sus datos ni ganar acceso a las funciones del sistema, y sin embargo

garantizar que esto no es denegado a personas y sistemas autorizados.

- Prevención de penetración o interferencia, ilegal o indeseada, de la operación apropiada o prevista de un sistema de control industrial.

- **Sistema de Gestión de la Seguridad de la Información:** (Inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

- **SoA:** Acrónimo inglés de Statement of Applicability. Véase: Declaración de aplicabilidad.

- **Tratamiento de riesgos:** (Inglés: Risk treatment). Proceso de modificar el riesgo, mediante la implementación de controles.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. DESARROLLO

INTRODUCCIÓN

El estándar para la seguridad de la información ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información), establece la necesidad de definir y documentar de acuerdo con la política de seguridad y privacidad de la información, las responsabilidades y roles de las personas que forman parte del sistema.

Dichos roles, se pueden agrupar en tres niveles principales según las funciones y el alcance. Estos niveles son:

- Nivel estratégico. El nivel estratégico toma decisiones alineadas con los objetivos del Instituto y elabora las directrices para encaminar al mismo en pro de la seguridad de la información. Este nivel está en cabeza del CIDA (Comité Institucional de Desarrollo Administrativo).

- Nivel táctico, Encargado de unir las decisiones estratégicas del Instituto con las labores diarias del nivel operativo, de tal manera que se escalen las necesidades operativas al nivel directivo y se interioricen las decisiones ejecutivas en todas las áreas del Instituto. Dicho nivel está en cabeza del líder del SGSI; a nivel organizativo las labores estarán en cabeza del Oficial de Seguridad de la información.

- Nivel operativo, Como su nombre lo indica, este nivel se encarga de todas las labores propias de los procesos habituales del Instituto y tiene un componente técnico. Ejecuta

todas las directrices creadas por el área estratégica y táctica y está en cabeza del oficial de seguridad del SGSI.

ESTADO ACTUAL A NIVEL ORGANIZATIVO EN LA OFICINA DE INFORMÁTICA EN EL IDEAM

En la actualidad, dentro de la estructura organizacional del IDEAM la Oficina de Informática es el área encargada de proveer los servicios de TI (infraestructura, hardware, software) en la entidad y de asesorar a las diferentes subdirecciones, oficinas y grupos en la adquisición, mantenimiento y desarrollo de herramientas informáticas.

La Oficina de Informática no cuenta en su interior con un organigrama definido y actualmente se definen ciertos grupos (no formales) de acuerdo a cada una de las responsabilidades y funciones que tiene frente a la entidad.

La Oficina de Informática cuenta con un grupo de especialistas y una mesa de servicios a través de un contrato de tercerización.

La información sobre cada uno de estos grupos se describe a continuación.

- **SISTEMAS DE INFORMACIÓN**

Sistemas de Información es el encargado de dar soporte a todos los sistemas de información que se encuentran en operación actualmente en el IDEAM.

✓ ***Funciones***

- Análisis, viabilidad técnica y priorización de requerimientos
- Conceptos técnicos en materia de sistemas de información
- Administración, mantenimiento y soporte de sistemas de información
- Coordinación y contratación de nuevos desarrollos de aplicaciones
- Planeación, seguimiento y control de los contratos cuyo objeto sea mantenimiento o desarrollo de nuevos aplicativos
- Verificación de la calidad de los productos asociados a desarrollo o mantenimiento de sistemas de información
- Definición y actualización de estándares de desarrollo
- Administración del modelo de datos
- Administración de la base de datos

✓ ***Roles***

Los roles identificados actualmente y que buscan asegurar una operación correcta de este grupo se describen a continuación: Lideres Técnicos (Administradores) de Sistemas de Información

- **INFRAESTRUCTURA TECNOLÓGICA**

El grupo de Infraestructura Tecnológica soporta la gestión de los componentes tanto a nivel de hardware como de software al interior de la entidad.

✓ ***Funciones***

- Inventario de hardware y software
- Conceptos técnicos en materia de infraestructura tecnológica
- Coordinación de soporte técnico
- Mantenimiento preventivo y correctivo de infraestructura tecnológica
- Administración de la red de datos
- Administración de infraestructura de seguridad (seguridad perimetral, dominio de red, ancho de banda, red interna, equipos de usuario)
- Adquisición y puesta en marcha de componentes de infraestructura (hardware, software, redes).
- Coordinación y contratación de adquisiciones o mantenimiento de infraestructura tecnológica

✓ ***Roles***

- Administrador de dominio
- Administrador de red LAN y WAN
- Administrador de imágenes satelitales
- Administrador de datos satelitales
- Administrador de banco de datos
- Ingenieros de soporte
- Administrador de sistema de seguridad perimetral
- Administrador de servidores
- Administrador de sistema de colaboración

- **SISTEMAS DE INFORMACIÓN GEOGRÁFICA**

El grupo de Sistemas de Información Geográfica es el encargado de soportar todos los sistemas de información con componente espacial que se encuentran en operación actualmente en el IDEAM.

✓ ***Funciones***

- Análisis , viabilidad técnica y priorización de requerimientos
- Conceptos técnicos en materia de Sistemas de Información Geográfica
- Administración, mantenimiento y soporte de sistemas de información con componente espacial
- Coordinación y contratación de nuevos desarrollos de aplicaciones con componente espacial

- Planeación, seguimiento y control de los contratos cuyo objeto sea mantenimiento o desarrollo de nuevos aplicativos con componente espacial
- Verificación de la calidad de los productos asociados a desarrollo o mantenimiento de sistemas de información con componente espacial
- Definición y actualización de estándares de desarrollo con componente espacial
- Administración del modelo de datos espacial (Vector y Raster) de la Geodatabase corporativa
- Administración de la aplicación para gestión de metadatos geográficos
- Soporte técnico en aplicaciones SIG
- Control y administración de las licencias SIG

✓ ***Roles***

- Líder Técnico Administrador de Sistemas de Información Geográfica

CONFORMACIÓN DE LA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL IDEAM

- **CONSIDERACIONES FRENTE A LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.**

Como parte de la definición del Sistema de Gestión de Seguridad de la Información del Instituto se recomienda una estructura de seguridad, con el fin de cumplir con lo establecido en la Norma ISO/IEC 27001:2013, en la Cláusula 5: Responsabilidad de la Dirección y en el Anexo A sección 6: Organización en la seguridad de la información, que incluye:

Objeto de Control

- A 6.1 Organización interna

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

Controles

A.6.1.1 - Roles y responsabilidades para la seguridad de la información
A.6.1.2 - Separación de Deberes
A.6.1.3 - Contacto con las autoridades
A.6.1.4 - Contacto con grupos de interés
A.6.1.5 Seguridad de la información en la gestión de proyectos

Objetivo de Control

- A.6.2 - Dispositivos Móviles y teletrabajo

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

Controles

A.6.2.1 - Política para dispositivos móviles
A.6.2.2 - Teletrabajo

A partir de estos controles podemos identificar el apoyo activo de la dirección del Instituto frente al tema de seguridad y la importancia que tiene la coordinación de todas las actividades de seguridad por los representantes de todas las partes involucradas dentro del alcance del SGSI; esto nos define que la organización de la seguridad debe involucrar a todo el Instituto, desde un alto nivel como lo es la dirección hasta el usuario final, pasando por los responsables de los procesos y la información. (Esto en el marco del alcance del SGSI).

- **ESTRUCTURA DE LA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL IDEAM**

Como punto de partida, se considera el componente sobre el cual se ha iniciado el enfoque en Seguridad de la Información en el IDEAM, a nivel de la Oficina de Informática y desde la cual se generarán los lineamientos y directrices hacia toda la entidad. La organización de la seguridad presenta la estructura y los roles del personal dentro de la Oficina de Informática con el objetivo de salvaguardar la seguridad de la información más relevante para la continuidad, cumplimiento legal y reglamentario sobre el cual se rige el Instituto; se definen las responsabilidades para el grupo encargado de coordinar los esfuerzos en seguridad de la información.

Los aspectos de responsabilidades en la Oficina de Informática deberán hacer parte de las actividades del día a día, de tal forma que la seguridad de la información se integre en la cultura de trabajo en cada uno de los funcionarios del Instituto, siempre realizando sus funciones con seguridad y protegiendo la información.

Una de las responsabilidades de la dirección del IDEAM y apoyada por la Oficina de Informática es asegurar la implementación y operación efectiva del Sistema de Gestión de Seguridad de la Información; como modelo de integración el Sistema de Gestión de Seguridad de la Información deberá unirse a los sistemas existentes en la actualidad en la entidad, con el fin de contar con un Sistema de Gestión Integrado.

Como parte integral del SGSI del IDEAM, es necesario definir una organización de seguridad de la información, la cual estará en cabeza del Comité Institucional de Desarrollo Administrativo, que tendrá un componente estratégico dentro del marco organizativo del Instituto.

La implementación y operación del SGSI es responsabilidad de todo el personal del Instituto y especialmente en la organización de la Oficina de Informática donde cumplen las funciones de brindar los servicios que requiere la entidad para ejercer su función.

A continuación, se define la organización de la seguridad del SGSI para el IDEAM, estableciendo los roles necesarios para la gestión del sistema en sus diferentes instancias.

- **COMITÉ INSTITUCIONAL DE DESARROLLO ADMINISTRATIVO**

El Comité Institucional de Desarrollo Administrativo (CIDA) conformado según resolución 223 del 2014, está integrado por un grupo interdisciplinario, que es la máxima autoridad en el tema dentro del Sistema de Gestión de Seguridad de la Información y asegurará el aspecto estratégico de la seguridad en el Instituto, brindando una clara dirección y apoyo para la implementación de las iniciativas relacionadas con seguridad.

Funciones del Comité Institucional de Desarrollo Administrativo para el SGSI.

Dentro de las funciones de este Comité están:

✓ ***Políticas, estándares y procedimientos***

- Validar y autorizar la implementación y operación del SGSI.
- Validar y aprobar la gestión de nuevos recursos para el SGSI para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el SGSI.
- Revisar la política del SGSI teniendo en cuenta las características del Instituto, la organización, su ubicación, sus activos y tecnología.
- Validar y aprobar el alcance y límites del SGSI en términos de las características del Instituto, la organización, su ubicación, sus activos y tecnología.
- Establecer las oportunidades de mejora y la necesidad de cambios del SGSI.
- La dirección debe aprobar, publicar y comunicar a todos los funcionarios y partes externas pertinentes, un documento de política de seguridad de la información.
- Aprobar las funciones y responsabilidades de seguridad de la información.
- Validar y aprobar una declaración de aplicabilidad propuesta por el líder del SGSI.

✓ ***Identificación, análisis, valoración, evaluación y tratamiento de riesgos***

- Validar y aprobar una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información identificada en el Instituto.
- Validar los niveles de riesgos residuales presentados por el Líder del SGSI.
- Definir los criterios para aceptación de riesgos, y los niveles de riesgo aceptables.
- Decidir sobre cualquier decisión o acción relacionada con la actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Validar y aprobar un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.

- Aprobar y revisar periódicamente las políticas y normas de seguridad de la información.

✓ ***Planeación estratégica de la seguridad***

- Conocer los planes y estrategias del Instituto.
- Aprobar y revisar los indicadores del Sistema de Gestión de la Seguridad de la Información.
- Validar y aprobar los planes de seguridad desarrollados.
- Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información.
- Dar a conocer los comunicados al Instituto que se refieren a la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua.

✓ ***Revisión y medición del SGSI.***

- Tener conocimiento sobre los resultados de las investigaciones sobre los incidentes de seguridad de la información.
- Tener conocimiento sobre procedimientos de seguimiento y revisión del SGSI.
- Tener conocimiento sobre revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

✓ ***Gestión de Activos***

- Validar las competencias necesarias para el personal que ejecute los trabajos en el SGSI.
- Asegurar que todo el personal al que se asigne responsabilidades definidas en el SGSI sea competente para realizar las tareas exigidas.

✓ ***Auditoría***

- Emprender revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, anomalías, medición de la eficacia, sugerencias y retroalimentación de todas las partes interesadas.
- Asegurar que se realizan auditorías internas del SGSI.
- Revisar los resultados de las auditorías realizadas al SGSI.

✓ ***Gestión de la continuidad del negocio***

El estándar NTC:ISO:22301 está enmarcado en la gestión de la continuidad del negocio, desde esta perspectiva se recomienda que debe existir un Sistema de Gestión de la Continuidad del Negocio. Teniendo en cuenta que la prioridad del Instituto actualmente está enfocada en la necesidad de implementar el SGSI, se describen algunas de las recomendaciones en continuidad de negocio bajo las recomendaciones descritas en la norma ISO 27001:2013

- Validar y autorizar la implementación y operación de los planes de continuidad de negocio.
- Validar y aprobar la gestión de recursos para la implementación de los planes de continuidad de negocio.
- Aprobar la política de continuidad de negocio teniendo en cuenta las características del Instituto, la organización, su ubicación, sus activos y tecnología.
- Validar y aprobar el alcance y límites de los planes de continuidad en términos de las características del Instituto, la organización, su ubicación, sus activos y tecnología.

✓ ***Gestión de vulnerabilidades***

- Aprobar el procedimiento de gestión de vulnerabilidades.

✓ ***Manejo de acciones preventivas y correctivas***

- Conocer las acciones que serán desarrolladas por los procesos para la remediación de las no conformidades u observaciones resultantes de las auditorias.

- **DISTRIBUCIÓN DE RESPONSABILIDADES PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.**

La organización diseñada para el IDEAM se generó teniendo como foco causar el mínimo impacto organizacional, en recursos humanos y desde luego económicos, logrando cumplir lo exigido normativamente.

El IDEAM se encuentra en un proceso de mejora continua en su sistema de gestión y de procesos, para ajustarse a las necesidades de la entidad y dar cumplimiento a las necesidades actuales y futuras de la prestación de sus servicios.

En este marco definido a manera de plan, se estructuran entonces los aspectos que deberán ser integrados en el IDEAM. El esquema propuesto lo que busca es que este trabajo se haga mediante la incorporación de los roles y responsabilidades de acuerdo a la estructura organizacional planteada, especialmente a nivel de los siguientes actores en la seguridad como se presenta en la Figura No. 3 Organización de la Seguridad IDEAM. Estos actores son:

- Comité Institucional de Desarrollo Administrativo
- Líder del SGSI
- Oficial de Seguridad

Para servir como apoyo de las decisiones que debe tomar el Comité Institucional de Desarrollo Administrativo, se contará con la participación de funcionarios de los Grupos de Apoyo dependiendo de la temática a normas o de los conceptos que se deseen emitir. Se establecen figuras como el Líder del SGSI encargado de coordinar las actividades de gestión de la seguridad de la información en la entidad y velar porque el proceso de seguridad de la información se

desarrollen en el marco del modelo propuesto, incorporando en las actividades del día a día (procesos y procedimientos) actividades tendientes a la protección de la información y a la ejecución de las actividades macro definidas dentro del modelo PHVA (Establecimiento, Operación, Mantenimiento, seguimiento y mejora).

Apoyando al Líder del SGSI en lo referente a los aspectos tecnológicos, se incorpora el rol de Oficial de Seguridad. Este tendrá la responsabilidad de establecer y definir lineamientos frente a la seguridad en los elementos tecnológicos que posee el Instituto de acuerdo a lo establecido a nivel del SGSI.

A continuación, se presentan las funciones de estos dos roles dentro del sistema.

- ✓ ***FUNCIONES DEL LÍDER DE SGSI***

El líder del Sistema de Gestión de Seguridad de la Información, permite la integración entre los aspectos estratégicos y los aspectos tácticos que se presenten en el SGSI. Es el representante del SGSI en el comité de seguridad y participa en las decisiones estratégicas.

Dentro de las funciones del Líder de Seguridad de la Información están:

Políticas, estándares y procedimientos

- Validar y proponer al comité el alcance y límites del SGSI en términos de las características del Instituto, la organización, su ubicación, sus activos y tecnología.
- Validar y proponer al comité la política de SGSI en términos de las características del Instituto, la organización, su ubicación, sus activos y tecnología.
- Validar la documentación del SGSI, desarrollada por el Oficial de Seguridad.
- Validar y presentar al Comité la declaración de aplicabilidad.
- Recomendar al Comité, sobre posibles actualizaciones de políticas, normas y estándares de seguridad de la información.

Identificación, análisis, valoración, evaluación y tratamiento de riesgos.

- Presentar al CIDA los componentes de la gestión del riesgo del SGSI.

Planeación estratégica de la seguridad

- Validar la implementación y operación del SGSI.
- Conocer y validar la implementación de programas de formación y toma de conciencia relacionados con el SGSI.
- Validar y presentar al CIDA los planes de seguridad desarrollados.
- Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información.
- Validar y aprobar el procedimiento de asignación de responsabilidades definidas en el

SGSI; para que todo el personal sea competente para realizar las tareas exigidas.

- Procurar la integración del Sistema de Gestión de Seguridad de la Información con los sistemas existentes en el Instituto con el objetivo de tener un Sistema de Gestión Integrado.

Revisión y medición del SGSI

- Conocer los procedimientos de seguimiento y revisión del SGSI.
- Conocer las revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia, sugerencias y retroalimentación de todas las partes interesadas.
- Validar el procedimiento para definir las acciones de gestión documental desarrolladas por el Oficial de seguridad.
- Validar la definición de la eficacia de los controles o grupos de controles seleccionados por las áreas.
- Conocer la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

Gestión de Activos

- Validar y proponer al CSI una metodología para la identificación, valoración, clasificación y tratamiento de los activos de información.
- Liderar la realización de la gestión de activos de información y riegos por parte del Instituto.
- Liderar la realización de análisis e investigaciones sobre los incidentes de seguridad de la información.
- Validar en el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

Auditoría

- Conocer la realización de auditorías internas al SGSI.
- Validar que se cumpla el establecimiento y mantenimiento de registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI.

Gestión de vulnerabilidades

- Solicitar al Comité de Seguridad de la Información los recursos necesarios para el desarrollo de la prueba de vulnerabilidades.
-
- Validar el plan de trabajo presentado por el Oficial de Seguridad para la realización de las pruebas.
- Solicitar al CSI los recursos necesarios para el desarrollo de los planes de remediación.
- Validar el plan de trabajo presentado por el Oficial de Seguridad para la realización de

los planes de remediación.
- Validar y presentar al CSI el procedimiento de gestión de vulnerabilidades.

Manejo de acciones preventivas y correctivas

- Validar y presentar al CSI las acciones preventivas y correctivas a ser tomadas para la remediación de las no conformidades u observaciones encontradas en las auditorias.
- Verificar que las no conformidades sean subsanadas.

Gestión de la arquitectura de seguridad

- Revisar y validar el diseño de arquitectura de seguridad definido por el Oficial de Seguridad.
- Solicitar al CSI los recursos necesarios para la implementación de la arquitectura de seguridad.
- Revisar los planes definidos para la implementación de la arquitectura.
- Comunicar formalmente a la Oficina de Informática el cronograma y el plan de trabajo para la implementación de la arquitectura.
- Verificar que el plan de implementación de la arquitectura se esté cumpliendo según lo definido.
- Evaluar los posibles cambios que se puedan presentar durante la implantación de la arquitectura.

Manejo de acciones preventivas y correctivas

- Validar y presentar al CSI las acciones preventivas y correctivas a ser tomadas para la remediación de las no conformidades u observaciones encontradas en las auditorias.
- Verificar que las no conformidades sean subsanadas.

Manejo de acciones preventivas y correctivas

- Validar y presentar al CSI las acciones preventivas y correctivas a ser tomadas para la remediación de las no conformidades u observaciones encontradas en las auditorias.
- Verificar que las no conformidades sean subsanadas.

Gestión de la arquitectura de seguridad

- Revisar y validar el diseño de arquitectura de seguridad definido por el Oficial de Seguridad.
- Solicitar al CSI los recursos necesarios para la implementación de la arquitectura de seguridad.
- Revisar los planes definidos para la implementación de la arquitectura.
- Comunicar formalmente a la Oficina de Informática el cronograma y el plan de trabajo para la implementación de la arquitectura.
- Verificar que el plan de implementación de la arquitectura se esté cumpliendo según

lo definido.
- Evaluar los posibles cambios que se puedan presentar durante la implantación de la arquitectura.

Continuidad de negocio

- Velar por la actualización de los planes de continuidad definidos por cada proceso.
- Gestionar la realización de las pruebas a los planes de continuidad.
- Apoyar a los procesos en la definición de sus planes de continuidad.
- Velar por la disponibilidad de los planes de continuidad de los procesos.
- Gestionar la documentación de los planes de continuidad de los procesos

Conocimientos y experiencia del Líder del SGSI

Conocimientos Mínimos

- Conocimientos avanzados en Sistemas de Gestión de la Seguridad de la Información.
- Modelos de Seguridad de la Información (Políticas, normas, estándares, procedimientos).
- Problemas de seguridad asociados a: servidores, bases de datos, aplicaciones.
- Conocimiento de seguridad en: bases de datos, sistemas operativos, aplicaciones, redes.
- Conocimiento en tecnologías de seguridad: firewalls, IDS2/IPS3, cifrado, antivirus, sistemas biométricos.
- Conocimiento básico de la legislación relacionada con seguridad de la información.

Conocimientos Deseados

- Conocimiento de estrategias de Seguridad de la Información.
- Cursos o charlas relacionadas con Seguridad de la Información.
- Conocimientos en modelos de Seguridad (Políticas, normas, procedimientos).

✓ ***FUNCIONES DEL OFICIAL DE SEGURIDAD***

El oficial de seguridad de la información se encarga de coordinar la ejecución de las actividades derivadas de la planeación, implementación, revisión y mantenimiento del SGSI. Coordina el aspecto táctico y operativo ejecutando las directrices del Comité de Seguridad de la Información y el Líder del SGSI.

[2] Sistema de Detección de Intrusos
[3] Sistema de Prevención de Intrusos

Dentro de las funciones del Oficial de Seguridad están:

Políticas, estándares y procedimientos:

- Definir y presentar al Líder del SGSI una declaración de aplicabilidad.
- Medir el nivel de cumplimiento de las políticas, estándares y procedimientos de seguridad de la información en el Instituto.
- Garantizar el establecimiento, mejora y actualización del manual del SGSI del Instituto.
- Definir cuáles son los estándares y procedimientos de seguridad de la información que debe tener el Instituto.
- Definir qué procedimientos van ser ejecutados por cuáles procesos o personas en el Instituto.
- Definir procedimientos junto con el grupo de Gestión de Calidad relacionados con pruebas de seguridad y de calidad a los diferentes sistemas de información y aplicaciones en la entidad.
- Definir procedimientos junto con el grupo de Infraestructura relacionados con la seguridad a nivel de la plataforma de hardware de la entidad.

Identificación, análisis, valoración, evaluación y tratamiento de riesgos.

- Definir y proponer al Líder del SGSI la metodología para la identificación, valoración, clasificación y tratamiento de los activos de información.
- Definir y proponer al Líder del SGSI una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del Instituto.
- Coordinar la realización de la gestión de identificación de riesgos realizada por las áreas.
- Coordinar la realización de la gestión de riesgos que incluye:
    - Análisis y evaluación de riesgos.
    - Identificación y evaluación de opciones para tratamiento de riesgos.
    - Selección de objetivos de control y controles para el tratamiento de riesgos.
- Recibir de las áreas responsables los riesgos residuales y presentarlos al Líder del SGSI.
- Consolidar la información sobre el plan de tratamiento de riesgos diseñado por las áreas responsables y presentarlo al Líder del SGSI.
- Coordinar la implementación del plan de tratamiento de riesgos de cada una de las áreas.
- Coordinar la implementación de controles seleccionados de cada área.
- Coordinar la realización de la revisión de las valoraciones de los riesgos a intervalos planificados, y el nivel de riesgo residual y riesgo aceptable identificado.
- Definir y proponer al Líder del SGSI los criterios para aceptación de riesgos, y los niveles de riesgo aceptables.

Planeación estratégica de la seguridad

- Definir y proponer al Líder del SGSI el alcance y límites del SGSI en términos de las características del Instituto, la organización, su ubicación, sus activos y tecnología.
- Validar la implementación y operación del SGSI.
- Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información.
- Garantizar la integración del Sistema de Gestión de Seguridad de la Información a los demás sistemas presentes en la entidad.

Revisión y medición del SGSI

- Coordinar la definición de la eficacia de los controles o grupos de controles seleccionados por las áreas.
- Coordinar y participar en el diseño de la implementación de programas de formación y toma de conciencia relacionados con el SGSI.
- Validar la necesidad de nuevos recursos para el SGSI para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI y presentarla al Líder del SGSI.
- Participar en el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Coordinar la realización de los procedimientos de seguimiento y revisión del SGSI.
- Coordinar la realización de la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Consolidar la información de las áreas sobre los planes de seguridad desarrollados y presentarla al líder del SGSI.
- Gestionar la documentación del SGSI en coordinación con el área encargada para esta labor.
- Gestionar el procedimiento para definir las acciones de gestión documental en coordinación con el área encargada para esta labor.
- Coordinar que se cumpla el establecimiento y mantenimiento de registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI con el área de procesos.
- Coordinar y participar en el diseño del procedimiento de asignación de responsabilidades definidas en el SGSI; para que todo el personal sea competente para realizar las tareas exigidas.
- Coordinar la realización de revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia, sugerencias y retroalimentación de todas las partes interesadas.
- Liderar la realización de análisis e investigaciones sobre los incidentes de seguridad de la información.

Gestión de Activos

- Liderar el proceso de identificación y valoración de activos de información más importantes del Instituto en términos de su confidencialidad, integridad y disponibilidad y atributos de manejo.
- Liderar el proceso de Clasificación de los activos de información del Instituto de acuerdo al esquema de clasificación y a los niveles de tratamiento definidos.
- Orientar la definición de procedimientos para el tratamiento de los activos de información.
- Definir un procedimiento de gestión de activos de información por medio del cual se opere un esquema de clasificación y tratamiento de la información del Instituto.
- Proponer los roles y responsabilidades en el Instituto requeridos para el manejo de la información.

Auditoria

- Coordinar la realización de auditorías internas al SGSI a intervalos planificados.

Gestión de la continuidad del negocio

- Apoyar a los procesos en la actualización de los planes de tratamiento.
- Apoyar a los procesos en la definición de sus planes de continuidad.
- Velar por la disponibilidad de los planes de continuidad de los procesos.
- Gestionar la documentación de los planes de continuidad de los procesos.

Gestión de vulnerabilidades

- Definir los planes y cronogramas para la realización de las pruebas de vulnerabilidades sobre la plataforma tecnológica del Instituto.
- Definir los cronogramas y planes para la remediación de las vulnerabilidades encontradas.
- Definir el procedimiento para la gestión de vulnerabilidades.
- Apoyar a los Grupos de Gestión de Infraestructura, Gestión de Sistemas de Información en el cierre de las vulnerabilidades identificadas en las pruebas de vulnerabilidad desarrolladas.

Manejo de acciones preventivas y correctivas

- Plantear acciones preventivas o correctivas, comunicar al área responsable y validar las acciones propuestas por las áreas.

Gestión de la arquitectura de seguridad

- Realizar el diseño de arquitectura de seguridad
- Proponer al Líder del SGSI, Jefe de la Oficina de Informática la arquitectura de seguridad de la información.
- Definir el plan para la implementación de la arquitectura.
- Verificar que el plan de implementación de la arquitectura se esté cumpliendo según lo definido.
- Junto con el líder de SGSI evaluar los posibles cambios que se puedan presentar durante la implantación.

Conocimientos y experiencia del Oficial de Seguridad de la Información

Conocimientos Mínimos

- Conocimientos avanzados en Sistemas de Gestión de la Seguridad de la Información.
- Modelos de Seguridad de la Información (Políticas, normas, estándares, procedimientos).
- Conocimiento en tecnologías de seguridad: firewalls, IDS/IPS, cifrado, antivirus, sistemas biométricos.
- Conocimiento en problemas de seguridad bases de datos, sistemas operativos, aplicaciones, redes.

Conocimientos Deseados

- Ser Auditor ISO/IEC 27001:2013.
- Ser Auditor ISO/IEC 22301:2012.
- Experiencia en desarrollo y administración de Modelos de Seguridad de la Información.
- Experiencia en el desarrollo de auditorías.
- Conocimiento de estrategias de seguridad de la información.
- Cursos y certificaciones relacionadas con Seguridad de la Información.

✓ ***Relación de la Organización de la Seguridad y el PHVA***

Como se puede observar con esta organización se busca que las responsabilidades sobre la seguridad de la información en el IDEAM se encuentran distribuidas a lo largo y ancho del Instituto (dentro de lo establecido a nivel del alcance). De esta forma se busca que el compromiso y actuación sobre el SGSI se establezcan desde los niveles más altos de dirección hasta los niveles más bajos de operación.

El Comité de Seguridad se torna como un ente orientado hacia dar la dirección y la definición de la estrategia para la implementación y operación del SGSI de la organización. Finalmente, los responsables de procesos y sus equipos de trabajo tendrán a su cargo responsabilidades más asociadas al día a día de la operación del SGSI.

6. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	23/12/2016	Creación del documento.
02	05/04/2018	Se actualiza, versión y codificación para cumplimiento con el decreto 415.

ELABORÓ:	REVISÓ:	APROBÓ:
Luis Alejandro Pinilla Oficial de Seguridad de la Información	Eduardo Ramirez Acosta Profesional Especializado Oficina Informática	Leonardo Cárdenas Chitiva Jefe Oficina Informática