Plan de

Seguridad y Privacidad de la Información

2024

IDEAM

Tabla de contenido

INTRODUCCIÓN

La información es un activo que tiene un alto valor para el Instituto y requiere en consecuencia una protección adecuada. Con base en el análisis de seguridad de la información se identificaron algunas vulnerabilidades, por lo que se emitió recomendaciones que contribuyen a mejorar el nivel de seguridad.

El Plan de Seguridad de la Información que se ha desarrollado se centra en la seguridad de los activos de información, de las personas y de los procesos del Instituto, salvaguardando la confidencialidad, integridad y disponibilidad mediante políticas que apalanquen la protección de la información y sea una guía para establecer las pautas que se deben cumplir al interior del Instituto (Sede Central), así como los integrantes del grupo de Seguridad de la Información.

El plan propone políticas que desarrollarán de acuerdo con los controles que se consideren necesarios, las cuales son la base para la implantación de instructivos y procedimientos.

El cumplimiento de las Políticas de Seguridad de Activos de Información es obligatorio. Ningún funcionario está exento del cumplimiento de estas políticas. Si un individuo del instituto viola las disposiciones en las Políticas de Seguridad de la Información, por negligencia o intencionalmente. El Instituto se reserva el derecho de tomar las medidas correspondientes, tales como acciones disciplinarias, despido, acciones legales, reclamo de compensación por daños, u otras1, tal como lo describe la política de seguridad y privacidad de la información.

OBJETIVO

Establecer un marco de acción para la implementación del Modelo de Seguridad y Privacidad de la Información, en atención al contexto organizacional de la entidad, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios y demás partes interesadas.

ALCANCE

La adopción del Modelo de Seguridad y Privacidad de la Información, para la vigencia 2023, se enfocará en fortalecer la implementación de acciones de acuerdo con los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados a la seguridad informática de la plataforma tecnológica y de la información del IDEAM, teniendo en cuenta las capacidades y recursos disponibles para mejorar la confianza de los ciudadanos, usuarios y demás partes interesadas.

Las políticas definidas en el presente plan de seguridad de la información aplican a todos los funcionarios, contratistas, pasantes y terceros que utilicen recursos del IDEAM. Estas políticas deben ser revisadas y en caso

[1] Ley 1273 de 2009: Ley de Delitos Informáticos

de necesitarse, actualizarlas periódicamente para garantizar que siguen siendo adecuadas, suficientes y eficaces para el sistema de gestión de seguridad de la información.

DEFINICIONES

- **Activo de Información:** La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades del instituto y, en consecuencia, necesita una protección adecuada.
- **Administrador de Dominio:** Persona encargada de administrar un conjunto de ordenadores (servidores + estaciones de trabajo) que comparten características comunes en cuanto a accesos.
- **Administrador de TI:** Profesionales encargados de operar y administrar la infraestructura tecnológica, comunicaciones, seguridad, aplicaciones y bases de datos del instituto.
- **Amenaza:** Causa potencial de un incidente no deseado, que pueda ocasionar daño a un sistema u organización.
- **Análisis de Impacto al Negocio:** Donde se determinan los recursos críticos y el tiempo de recuperación con las respectivas ventanas de criticidad mediante las cuales se debe restaurar los activos evaluados.
- **Análisis del Riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Aplicación:** Es un tipo de programa Informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo.
- **Ataque:** intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo.
- **Cifrar:** quiere decir transformar un mensaje en un documento no legible.
- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para quienes están autorizados.
- **Contratista:** Persona jurídica o natural externa al Instituto encargada de adelantar actividades por encargo del instituto.
- **Cuenta de acceso:** Identificación y contraseña a través de la cual un usuario accede a un servicio o aplicación. Las cuentas de acceso son autorizadas por los Jefes de las diferentes dependencias y suministradas por los Administradores de los servicios o aplicaciones y está sujeta a la disponibilidad de licencias adquiridas por el Instituto.
- **Custodio:** Encargado de guardar el activo con cuidado y vigilancia. Es una parte designada del instituto, un cargo, proceso, o grupo de trabajo encargado de administrar los componentes tecnológicos donde se encuentra la información; además se encarga de hacer efectivos los controles de seguridad administrativos que el propietario de la información haya definido, tales como el manejo de archivos, el uso de copias y la eliminación.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.
- **Incidente de Seguridad de la Información:** Un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad:** Salvaguarda de la exactitud y completitud de la información y sus métodos de procesamiento.

- **Política:** Son instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.
- **Propietario:** El término "Dueño" o "Propietario" identifica a un individuo o a un instituto que tiene responsabilidad aprobada por la Dirección por el control de la producción, el desarrollo, elmantenimiento, el uso y la seguridad de los activos. El término "Propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.
- **Recurso Informático:** Cualquier componente físico (Hardware) o lógico (Software) empleado para almacenar, manipular, procesar o transmitir información del IDEAM.
- **Requerimiento:** es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Se usa en un sentido formal en la ingeniería de sistemas o la ingeniería de software.
- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.
- Rol: Grupo de usuarios que cumplen un papel determinado, a los cuales se les asigna o niega permisos dentro de un aplicativo.
- **Servidor:** un computador que ofrece servicios a máquinas de cliente distantes o a aplicaciones, como el suministro de contenidos de páginas u otros recursos.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas [ISO/IEC 27001:2005].
- **Servicio o Aplicación:** Programa o conjunto de programas diseñados para la realización de una(s) tarea(s) concretas. Los servicios están destinados principalmente para apoyar los diferentes procesos del Instituto. Por ejemplo, correo electrónico, Internet, SISAIRE, SNIF, SIORH, etc.

METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD

CICLO OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital observa el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información2.

[2] Modelo de Seguridad y Privacidad, MINTIC, Pág. 7-8 https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

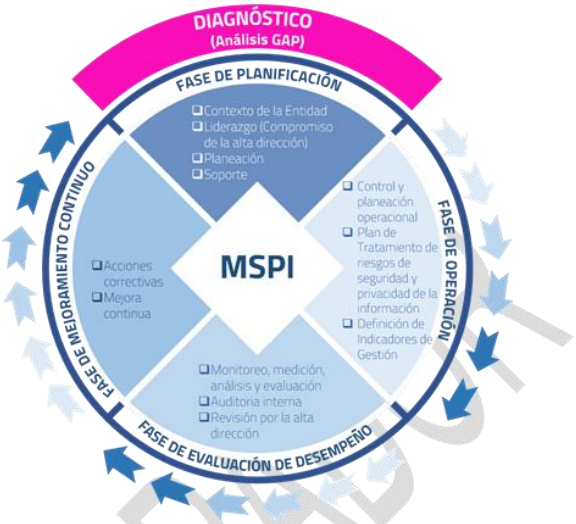
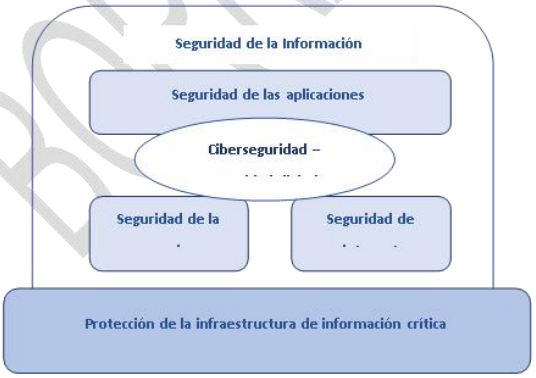


Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información



Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)
Fuente: Documento Modelo de Seguridad y Privacidad de la Información V.4 MINTIC

- **Fase Diagnostico:** Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
- **Fase Planificación (Planear):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (Hacer):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (Verificar):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Mejora Continua (Actuar):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACIÓN

La ISO/IEC 27001:2013 adapta con una serie de lineamientos que sirven para el desarrollo de un sistema de gestión de la seguridad de la información, que sin importar el tipo de empresa, se pueda alinear con otros sistemas de gestión en la empresa. Esta nueva estructura propuesta, alineada con el ciclo de la Mejora Continua tiene la siguiente estructura: Norma ISO 27001:2013 alineado al Ciclo de mejora continua

Fuente: https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento cuatrimestral.

FASE I: ANÁLISIS DE BRECHA	
ANÁLISIS GAP ISO 27001 y MSPI	
Objetivo	**Actividades**
Elaborar el análisis GAP (análisis de brecha) frente a la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información del IDEAM	Identificar y entender el contexto interno y externo del IDEAM, partes interesadas y factores críticos de éxito
	Realizar entrevistas y recopilación de documentación con las personas responsables en los procesos de ejecutar las actividades contempladas en los controles, para identificar la forma como se ejecutan actualmente dichos controles
	Realizar un análisis GAP o de brecha al SGSI, siguiendo como marco de referencia la norma ISO 27001:2013, a fin de establecer el nivel d cumplimiento de la misma de acuerdo con el alcance definido por el IDEAM y establecer el estado deseado del sistema

FASE II: ESTABLECIMIENTO DEL SGSI	
DISEÑO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD	
Diseñar y/o actualizar políticas y procedimientos de seguridad conforme la estructura propuesta por la norma ISO 27001:2013 alineados al Sistema Integrado de Gestión de la Entidad	Actualizar el manual de políticas y procedimientos respetando la estructura propuesta por la norma ISO 27000.
	Elaborar y actualizar las políticas y procedimientos alineado a lo exigido por la norma ISO 27001:2013 y por MPSI.
	Definir y documentar formalmente el proceso de gestión de incidentes del SGSI
	Crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información.

FASE III: ANÁLISIS DE RIESGOS	
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN	
Objetivo	**Actividades**
Identificar los activos de información de los procesos de Negocio IDEAM incluidos en el alcance.	Realizar la actualización de los activos de información
	Actualización de matriz de riesgos
	Realizar el Registro Nacional de Base de Datos

FASE IV: PRUEBAS DE SEGURIDAD	
HACKING ÉTICO Y INGENIERIA SOCIAL	
Objetivo	**Actividades**
Identificar las vulnerabilidades que existen dentro de la configuración física y lógica de los sistemas informáticos de la Entidad. (esta actividad se requiere ser elaborada por terceros) .	HACKING ÉTICO: • Recolección de información. • Identificación de sistemas y servicios. • Identificación y verificación de vulnerabilidades. • Presentaciones informes de resultados.
	INGENIERÍA SOCIAL: • Determinar entre las partes el perfil de los funcionarios y contratistas a los cuales se les debe realizar pruebas de ingeniería social • Elaboración de los instrumentos y herramientas a utilizar de acuerdo con el perfil de los empleados a evaluar y las pruebas aprobadas • Realización de las pruebas de ingeniería social • Análisis de resultados

FASE V: ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN	
CAMPAÑAS Y CAPACITACIONES EN SEGURIDAD	
Objetivo	**Actividades**
Realizar las capacitaciones a los funcionarios y contratistas de la Entidad.	Realizar la actualización del plan de sensibilización de seguridad de la Información con las capacitaciones y campañas de seguridad a realizar en la vigencia.
	Realizar una evaluación que permita medir el conocimiento asimilado por los funcionarios capacitados en temas de seguridad informática.
	Socializar el informe del proceso de entrenamiento de seguridad de la Información.

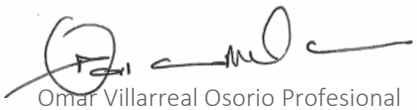
FASE VI: SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN	
AUDITORIA INTERNA SGSI	
Objetivo	**Actividades**
Realizar las capacitaciones a los funcionarios y contratistas de la Entidad.	Desarrollar actividades preparatorias que busquen orientar al IDEAM para afrontar el proceso de auditoría.
	Realizar la recolección de evidencia suficiente y probatoria sobre el cumplimiento de los requisitos que exige la norma ISO 27001:2013.
	Desarrollar el informe y recomendaciones del proceso.

HOJA DE RUTA

Para cada una de las fases planteadas para la vigencia 2024 se establecen las fechas de culminación de la misma con la cantidad de entregables.

FASES	2024											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
FASE I				1								
FASE II				2			2			2		
FASE III						3						
FASE IV							1				1	
FASE V						2					1	
FASE VI											1	

VERSIÓN	FECHA	DESCRIPCIÓN
001	14/02/2013	Creación del documento.
002	25/11/2015	Actualización del documento.
003	29/11/2017	Actualización documento para SGI
004	11/04/2018	Actualización del documento y para dar cumplimiento al decreto 415
005	21/09/2018	Actualización documento. Política 1 y 6
006	11/10/2018	Actualización documento. Política 6
007	18/12/2019	Creación de la Política 16
008	25/01/2021	Inclusión plan y cronograma de seguridad y privacidad de la información
009	17/01/2022	Actualización cronograma de seguridad y privacidad de la información
010	03/01/2023	Actualización del documento en su cronograma de seguridad y privacidad de la información
011	29/12/2023	Actualización del documento en su estructura y cronograma

ELABORÓ:	REVISÓ:	APROBÓ
 Omar Villarreal Osorio Profesional Especializado Grupo GAESI	 Juan David García Castaño Jefe Oficina Informática	 Juan David García Castaño Jefe Oficina Informática