PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Gestión Tecnológica y Comunicaciones

ENERO DE 2023

INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL - INFOTEP

Av. Colombia, Barrio Sarie Bay

Datos de Contacto:

Institución	INSTITUTO NACIONAL DE FORMACIÓN TECNICA PROFESIONAL - INFOTEP
NIT	892400461-5
Rector	Silvia Montoya Duffis
Documento preparado por	Ing. Jonathan Marín Medicis
Conmutador	+57 8 5125770 - +57 8 5126607
Fax	+57 8 5123350
Código DANE	88001 – nit: : 892000000-0
Correo Notificaciones Judiciales	notificacion@infotepsai.edu.co
Correo contacto y PQRD	info@infotepsai.edu.co – serviciocliente@infotepsai.edu.co
Sitio Web	www.infotepsai.edu.co
Horario de Atención al Público	lunes a viernes 8:00 am a 12:00 pm y de 3:00 pm a 7:00 pm
Dirección	Avenida Colombia, Barrio Sarie Bay. San Andrés Isla, Colombia

INTRODUCCIÓN

En la actualidad, la información es uno de los activos más valiosos para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible, integra y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

La seguridad informática es hoy en día una disciplina y una práctica que toda organización sin importar su dimensión (Grande, Medina o Pequeña), debe desarrollar intrínsecamente con el fin blindar las operaciones que se apalanquen a través de la infraestructura tecnológica con la que se dispone.

Las entidades deben ser conscientes de todo el tipo de amenazas existentes que podrían atentar contra la seguridad y privacidad de la información, lo cual representa un riesgo que si llegara a materializarse podría llegar a parar la operación causando pérdidas económicas, sanciones legales, afectación de imagen y reputación. Por tal motivo la seguridad de la información cada día más forma parte de los planes estratégicos de las entidades. Por lo tanto es importante que los encargados de la seguridad de la información estén constantemente implementando y mejorando las medidas de seguridad orientadas a prevenir los riesgos y amenazas que pueden llegar a comprometer la información.

Es importante que las entidades realicen una correcta identificación, análisis, valoración y administración de los riesgos relacionados con la seguridad de la información que pueden afectar los objetivos institucionales. Con el propósito de implementar medidas y controles que permitan una adecuada gestión de situaciones que pongan en riesgo la información.

TABLA DE CONTENIDO

1. OBJETIVO

Definir las actividades del plan de Seguridad y Privacidad de la Información para la implementación, gestión, verificación y mejora continua del Sistema de Gestión de Seguridad de la Información, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea y las necesidades de la entidad.

2. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información del Instituto Nacional de Formación Técnica Profesional INFOTEP de San Andrés Islas aplica a toda la entidad, procesos, sus funcionarios, estudiantes, contratistas y terceros del INFOTEP y la ciudadanía en general.

3. DEFINICIONES

Para efectos de la comprensión del plan de seguridad de la Información del Instituto Nacional de Formación Técnica Profesional, se establecen los siguientes significados de las palabras empleadas en el texto:

- **Seguridad de la Información:** se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. (ISO27001)
- **Políticas:** directrices u orientaciones por las cuales la alta dirección define el marco de actuación con el cual se orientará la actividad pública en un campo específico de su gestión, para el cumplimiento de los fines constitucionales y misionales de la entidad, de manera que se garantice la coherencia entre sus prácticas y sus propósitos.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

4. METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD

La estrategia de Gobierno Digital contempla un ciclo de operación de 5 fases, con las cuales de ser aplicadas por la entidad le permitiría gestionar adecuadamente la seguridad y privacidad de sus activos de información.

- **Fase Diagnostico**: Esta fase permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- **Fase Planificación (P**lanear**):** Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.
- **Fase Implementación (H**acer**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (V**erificar**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

- **Fase Mejora Continua (A**ctuar**):** 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.

5. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

La dirección de INFOTEP, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.
Para INFOTEP, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.
De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de INFOTEP.
- Garantizar la continuidad del servicio frente a incidentes.
- INFOTEP ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la institución, y a los requerimientos regulatorios.

6. OBEJTIVOS DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN

- Administrar los eventos de seguridad de la información del INFOTEP.
- Fortalecer la seguridad y disponibilidad de la información y plataforma tecnológica.
- Cumplir con los requisitos legales aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.
- Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios, contratistas y estudiantes).
- Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

7. ALCANCE DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION

EL SGSI es aplicable a los activos de información de todos los procesos del INFOTEP, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información.

8. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Con el objetivo de la entidad de implementar el sistema de gestión de seguridad de la información- SGSI se definieron las siguientes actividades para el 2023 con las cuales se estable el plan de seguridad y privacidad de la información.

8.1 Fase de diagnostico

OBJETIVO: Identificar el estado de la entidad con respecto a los requerimientos del Modelos de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital.

Actividad	Fecha Inicio	Fecha Final	Responsable
Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC	20/02/23	20/02/23	Jonathan Marín Medicis
Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de	20/02/23	20/02/23	Jonathan Marín Medicis

información de la entidad y definición de planes de mitigación			
Recolección de información con el fin de conocer todo lo existente en temas de seguridad que ya tenga la institución.	20/02/23	20/02/23	Jonathan Marín Medicis

8.2 Fase de planeación

A continuación, se dan a conocer las actividades definidas para en la etapa de planeación para la implementación del Sistema de Seguridad de la Información en la vigencia 2023.

Actividad	**Fecha Inicio**	**Fecha Final**	**Responsable**
Realizar un análisis de toda la documentación existente en la entidad en temas de seguridad de la información.	20/02/23	20/02/23	Jonathan Marín Medicis
Actualizar el alcance del SGSI de la entidad	20/03/23	20/03/23	Jonathan Marín Medicis
Actualizar las políticas de seguridad y privacidad de la información de la entidad	20/03/23	20/03/23	Jonathan Marín Medicis
Actualizar Roles y Responsabilidades para la implementación y gestión de seguridad de la información.	20/03/23	20/03/23	Jonathan Marín Medicis
Actualizar documentos para el apoyo de la operación tales como formato de procesos y procedimientos del sistema de seguridad de la información.	20/04/23	20/04/23	Jonathan Marín Medicis
Actualizar y Gestionar los activos de información.	20/04/23	20/04/23	Jonathan Marín Medicis
Actualizar la identificación, valoración y tratamiento de riesgos.	20/05/23	20/05/23	Jonathan Marín Medicis
Actualizar el plan de capacitación, comunicación y sensibilización de seguridad de la información.	20/05/23	20/05/23	Jonathan Marín Medicis
Realizar el plan de diagnóstico de IPv4 a IPv6	20/06/23	20/06/23	Jonathan Marín Medicis

8.3 Fase de implementación

OBJETIVO: Llevar a cabo la implantación de la planificación realizada en la fase de planeación del Modelo de Seguridad y Privacidad de la Información.

Actividad	Fecha Inicio	Fecha Final	Responsable
Implementar el plan de implantación del MSPI.	20/07/23	20/07/23	Jonathan Marín Medicis
Implementación del plan de tratamiento de riesgos.	20/07/23	20/07/23	Jonathan Marín Medicis
Establecer los indicadores de gestión	20/08/23	20/08/23	Jonathan Marín Medicis
Ejecutar el plan de transición de IPv4 a IPv6.	20/08/23	20/08/23	Jonathan Marín Medicis

8.4 Fase de evaluación de desempeño

OBJETIVO: Evaluar el desempeño y la eficacia del SGSI, en base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Actividad	Fecha Inicio	Fecha Final	Responsable
Plan de revisión y seguimiento, a la implementación del MSPI.	20/09/23	20/09/23	Jonathan Marín Medicis
Plan de Ejecución de Auditorias	20/09/23	20/09/23	Jonathan Marín Medicis

8.5 Mejora continua

OBJETIVO: Consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información.

Actividad	Fecha Inicio	Fecha Final	Responsable
Diseñar el plan de mejoramiento	20/11/23	20/11/23	Jonathan Marín Medicis

9. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

10. SEGUIMIENTO

Para hacer seguimiento al Plan de de Seguridad y Privacidad de la Información se deberá tener en cuenta lo siguiente y se consignará en el formato dispuesto para realizar esta actividad

Nombre del Indicador	Medición/Expresión del Indicador	Frecuencia	Meta Programada	Responsable
Implementación de MSPI	Implementación de MSPI	No actividades ejecutadas /No actividades programadas X 100 (MSPI)	30%	Area de Sistemas

Ver cronograma del plan de implementación del MSPI – 2023

CRONOGRAMA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FASE	ACTIVIDADES / ESTRATEGIAS	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE				Totales		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	Realizadas	Pendientes	Aplazadas
DIAGNÓSTICO	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	0k	0k																																													X		
	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad			0k	0k																																											X		
	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.			0k	0k																																											X		
	Revisión y Actualización																																																	
PLANEACIÓN	Actualizar Política y manual de Seguridad y Privacidad de la Información																					0k																												X		
	Revisar y aprobar Política de Seguridad																																																X		
	Elaborar procedimientos de seguridad de la información:																																																	
	* SEGURIDAD DEL RECURSO HUMANO																					0k																												X		
	* GESTION DE ACTIVOS																					0k																												X		
	* CONTROL DE ACCESO																					0k																												X		
	*CRIPTOGRAFÍA																						0k																											X		
	* SEGURIDAD FÍSICA Y DEL ENTORNO																						0k																											X		
	* SEGURIDAD DE LAS OPERACIONES																																																	
	* SEGURIDAD DE LAS COMUNICACIONES																																																	
	* ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN																								0k																								X		
	* GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN																								0k																								X		
	* ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO																																																
	Definir los Roles y responsabilidades de seguridad y privacidad de la información.																																																
	Aprovación de acto administrativo																																																
	Realizar el inventario de activos de información.																										0k	0k																						X		
	Realizar la Integración del MSPI con el Sistema de Gestión documental																																																
	Realizar la Identificación, Valoración y tratamiento de riesgo.																																															X		
	Realizar el plan de Comunicaciones.																																															X		
	Realizar el plan de diagnóstico de IPv4 a IPv6.																														0k																	X		
IMPLEMENTACIÓN	Planificación y Control Operacional.																																																
	Implementar el plan de tratamiento de riesgos.																																																	71% NOV
	Implemetar el plan de comunicaciones																																																81 DIC
	Definir Indicadores De Gestión.																																																
	Implementar el plan de Transición de IPv4 a IPv6																																																
FASE DE EVALUACIÓN DE DESEMPEÑO	Plan de revisión y seguimiento, a la implementación del MSPI.																																																
	Plan de Ejecución de Auditorias																																																
	Realizar seguirmiento a los controles de seguridad de la información																																																
	Auditoria de seguridad de la información																																																
FASE DE MEJORA CONTINUA	Impelemntacion de planes de mejoramiento y revisiones por la alta dirección																																																