PLAN DE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA

INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL

Humberto Velásquez García

INFOTEP

Ciénaga – Magdalena

CONTENIDO DEL DOCUMENTO Pag.

1. INTRODUCCIÓN.

Considerando los procesos de mejora que se han llevado a cabo en la institución, producto de la puesta en marcha del Sistema Integrado de gestión de la calidad, así como los relacionados con el Sistema de aseguramiento de la Calidad, los cuales, hoy se soportan en poderosas herramientas de software, que han permitido hacer ágiles los procedimientos y actividades de cada uno de los procesos (Estratégicos, Misionales, de apoyo y de evaluación), posibilitando la generación oportuna de información, y con ésta, la toma oportuna de las decisiones, por parte de la alta dirección, que contribuye a implementar las acciones preventivas, correctivas y de mejoramiento apropiadas, buscando incrementar la satisfacción de los clientes y demás partes interesadas.

En este sentido, y teniendo en cuenta la importancia que para la institución posee la información, como su activo fundamental, se hace necesario que se establezca, implemente y se mantenga un Modelo que permita gestionar, de buena manera, la seguridad y privacidad de la información generada desde cada proceso, así como la información, actual e histórica, de docentes, estudiantes, personal administrativo, egresados, proveedores y demás partes interesadas, debido a las diferentes amenazas y riesgos a los que esta se encuentra expuesta, dados las diferentes amenazas y riesgos de los sistemas informáticos, producto de los continuos ataques perpetrados por parte de delincuentes físicos y virtuales, que se valen de diferentes medios, para robar o exponer información crítica de las empresas, organizaciones e instituciones.

Por lo anterior, las directivas de la IES INFOTEP, apoyándose en las directrices establecidas por el gobierno nacional, a través del Ministerio de las tecnologías de la información y la comunicación, en el marco de lo que han denominado la política de Gobierno digital, ha decido iniciar las actividades pertinentes para la construcción y puesta en funcionamiento de un Modelo de Seguridad y privacidad de la información, para lo cual, iniciará realizando un diagnóstico que le permita determinar el estado actual, y en qué etapa del modelo se encuentra, la seguridad y privacidad de la información en la institución, cuyo resultado sentará las bases para diseñar un plan de seguridad y privacidad de la información, en el que se establecerán los tiempos, fases y actividades para implementar el modelo en la Institución, en el corto, mediano y largo plazo.

2. OBJETIVO.

Trazar y planificar los procedimientos y actividades que la IES INFOTEP requiere para la realización e implementación del Plan de Seguridad y Privacidad de la Información - PSPI, el cual, le permitirá establecer políticas y lineamientos para la salvaguarda de la información y sus activos de información, y su uso adecuado.

3. ALCANCE.

El alcance del Plan de Seguridad y Privacidad de la Información – PSPI, aplica para todos los procesos del sistema de gestión de la calidad de la IES INFOTEP, así como para los docentes, personal administrativo y contratistas.

4. JUSTIFICACIÓN.

La justificación del PSPI de la IES INFOTEP de Ciénaga, Magdalena, se sustenta en la importancia que en la actualidad posee para la IES INFOTEP, la información y los activos de información, como eje para su funcionamiento, cumplimiento en la generación de reportes, así como en la satisfacción de los clientes y demás partes interesadas. Así mismo, se justifica en lo establecido en:

- La constitución Política de Colombia 1991. En su artículo 15, en el que se reconoce como derecho fundamental el habeas Data, y el artículo 20, en lo pertinente a la libertad de información.
- La Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- El Decreto Único Reglamentario del sector de las Tecnologías de la Información y las comunicaciones 1078 de 2015.
- El Decreto 612 de abril de 2018, a través del cual se fijan las directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del estado.
- El Decreto 1008 de junio de 2018, por medio del cual se establecen los lineamientos generales de la política de Gobierno digital.
- La Norma Técnica Colombiana NTC/ISO 27001:2013, que detalla el Sistema de Gestión de la Seguridad de la Información.
- El Modelo de Seguridad y privacidad de la Información del Ministerio de Tecnologías y Sistemas de información.
- Los lineamientos para la Administración del riesgo (L-DE-01).

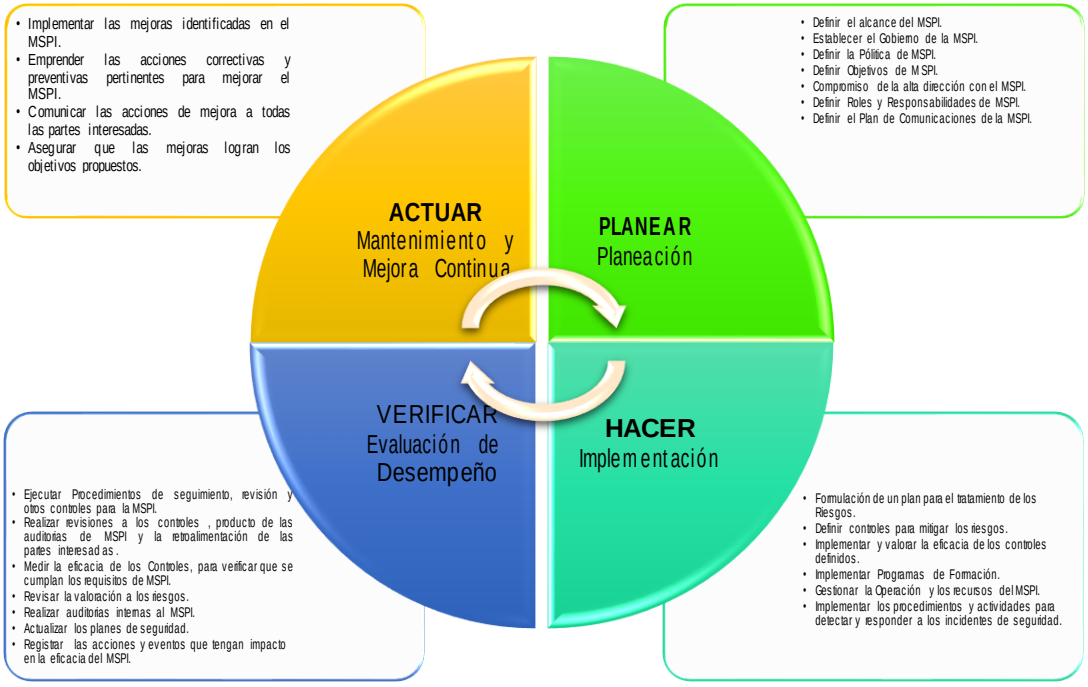
- Guía para la formulación, seguimiento y evaluación de planes de mejoramiento (G-EM-01).
- El manual de políticas de seguridad de la información (M-TI-01).
- La dimensión de información y comunicación del Modelo Integrado de Planeación y Gestión (Decreto 1499 de 2017)

PRESENTACIÓN DE LA INSTITUCIÓN.

La IES INFOTEP, es una Institución de Educación Superior, del orden departamental, de carácter oficial y con régimen autónomo, dedicada a la docencia, la investigación, la extensión, y el análisis de los problemas de la Región Caribe y el País, cuyo objeto, es el de formar y capacitar ciudadanos íntegros, mediante el ofrecimiento de programas de formación técnica profesional, tecnológica y profesional universitaria, así como programas de formación para el trabajo y de especialización en su respectivo campo de acción, buscando dar respuesta a las necesidades del sector productivo, social y cultural de nuestro entorno.

5. CICLO DE OPERACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El ciclo de operación para la realización e implementación del MPSI de la IES INFOTEP de Ciénaga, está estructurado en cuatro etapas fundamentales, la primera de Planeación, la segunda de implementación, la tercera de evaluación de desempeño, y la última, de Mantenimiento y Mejora, las cuales se alinean con el Modelo para la mejora continua, denominado ciclo de Deming, que es una estrategia para la mejora continua de la calidad, que consiste en cuatro pasos o fases a saber: PHVA (Planificar, Actuar, verificar, Hacer). Es así como a continuación se presenta la figura en la que se ilustra, el modelo para la realización e implementación del MSPI y su alineación con el Modelo PHVA:



5.1. FASE DE DIAGNÓSTICO DEL ESTADO ACTUAL DE LA INSTITUCIÓN CON RESPECTO A LOS COMPONENTES DEL LA NORMA ISO 27001:2013 Y EL MSPI DEFINIDO POR MINTIC.

En este aparte es preciso destacar, que el soporte del ciclo de operación del MPSI, se sustenta en una fase previa, en la que se realizó un diagnóstico de la situación actual de la seguridad y la privacidad de la información en la IES INFOTEP, para lo cual, se utilizó y aplicó una herramienta de diagnóstico de la seguridad y privacidad de la información, proporcionada por el Ministerio de las Tecnologías de la Información y las comunicaciones, que busca brindar apoyo a las instituciones, para que puedan realizar un análisis de brechas, que les permitirá determinar, cómo se encuentran actualmente, frente a los controles del estándar ISO 27001:2013, y la guía de controles del MSPI, y de esta forma implementar un Plan para la realización en implementación del MSPI.

En este sentido, luego de analizar y calificar los componentes de la herramienta diagnóstica de MINTIC, se logró establecer, que la institución posee brechas significativas frente a las exigencias establecidas en la herramienta, como se puede observar en la siguiente tabla y la gráfica correspondiente:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	9	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	6	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	0	100	INEXISTENTE
A.9	CONTROL DE ACCESO	5	100	INICIAL
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	4	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	3	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	7	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	17	100	INICIAL
A.18	CUMPLIMIENTO	11,5	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		6	100	INICIAL

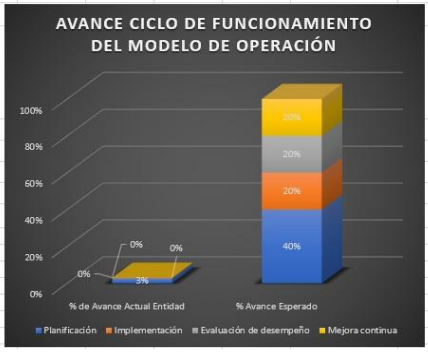
Luego de observar y analizar la tabla y la gráfica se evidencia que el promedio de la evaluación realizada a los controles es de 6, lo que indica que la institución, al verificar en la tabla de los valores de nivel de madurez, se encuentra en un nivel de madurez INICIAL, como se observa a continuación:

NIVEL DE MADUREZ MSPI	
Nivel	**Descripción**
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información

En lo que corresponde a la calificación obtenida por la institución, frente al avance en los componentes de la herramienta relacionados con el modelo de operación PHVA, es decir, con los de la Planificación (Planear), la Implementación (Hacer), la evaluación del Desempeño (Verificar), y la Mejora Continua (Actuar), se evidencia que la institución obtuvo una calificación muy baja, del **3%**, con respecto a un porcentaje de avance del 40% establecido en la herramienta, evidenciando un rezago importante, lo que la obliga a dar inicio y culminar, en este año 2019, el proceso de Planificación del modelo, y llevarlo al 40% exigido, para que en el 2020, inicie y consolide la implementación del MSPI. La calificación en el avance PHVA de la IES INFOTEP, se puede observar a continuación:

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2019	Planificación	3%	40%
2020	Implementación	0%	20%
2021	Evaluación de desempeño	0%	20%
2022	Mejora continua	0%	20%
TOTAL		3%	100%



La aplicación y calificación de los componentes de la herramienta diagnóstica suministrada por MINTIC, se convirtió en un insumo fundamental para que la IES INFOTEP, lograra establecer sus debilidades y las brechas existentes frente al MSPI, y de esta manera, elaborar el Plan para la realización e implementación del Modelo de Seguridad y Privacidad de la Información.

5.2. FASE DE PLANEACIÓN DEL MSPI.

Para los fines de esta fase, fue de gran importancia el análisis de los resultados obtenidos luego de la aplicación de la herramienta para diagnosticar el estado actual de la institución frente al MSPI, en el que se logró evidenciar las grandes brechas que posee la institución frente a cada uno de los

componentes definidos para el modelo de la herramienta, por lo cual, esta fase es de suma importancia para dar inicio a la realización e implementación exitosa del MPSI en la IES INFOTEP de Ciénaga, Magdalena, por lo tanto, se hace necesario definir y establecer en esta fase:

- el alcance del MSPI,
- el Gobierno de la SPI,
- la Política de SPI,
- el Objetivos de SPI,
- el Compromiso de la alta dirección con el MSPI,
- los Roles y Responsabilidades de SPI, y
- el Plan de Comunicaciones de la SPI.

FASE DE IMPLEMENTACIÓN DEL MSPI.

Para llevar a cabo esta fase, es necesario que se complete a cabalidad con la fase de planificación, del ciclo de operación del MSPI, lo que permitirá a la IES INFOTEP, la implementación de los aspectos, actividades y planes requeridos por el MSPI, por lo que, en esta fase, se deben llevar a cabo en el mediano plazo, los siguientes aspectos:

- La Formulación de un plan para el tratamiento de los Riesgos.
- Definir controles para mitigar los riesgos.
- Implementar y valorar la eficacia de los controles definidos.
- Implementar Programas de Formación.
- Gestionar la Operación y los recursos del MSPI.
- Implementar los procedimientos y actividades para detectar y responder a los incidentes de seguridad.

5.3. FASE DE EVALUACIÓN DEL DESEMPEÑO DEL MSPI.

Para el desarrollo y éxito de esta fase, se hace necesario que se evalúe, y en donde sea pertinente, medir el desempeño del proceso, frente a la política y los objetivos de la Seguridad de la Información, así como la experiencia práctica, con el fin de reportarlos a la alta dirección para su revisión, por lo tanto, se hace necesario que se lleven a cabo los siguientes aspectos fundamentales:

- Ejecutar Procedimientos de seguimiento, revisión y otros controles para la SPI.

- Realizar revisiones a los controles, producto de las auditorias de SPI y la retroalimentación de las partes interesadas.
- Medir la eficacia de los Controles, para verificar que se cumplan los requisitos de SPI.
- Identificar y revisar la valoración de los riesgos y amenazas.
- Realizar auditorías internas al MSPI.
- Actualizar los planes de seguridad.
- Registrar las acciones y eventos que tengan impacto en la eficacia del MSPI.

5.4. FASE DE MANTENIMIENTO Y MEJORA DEL MSPI.

En este punto, se deben emprender las acciones correctivas y de mejoramiento, basándonos en los resultados de las auditorías internas del MSPI y los emitidos por la revisión realizada por la dirección, lo que permitirá lograr la mejora continua del MSPI de la IES INFOTEP. Por tanto, se deben llevar a cabo las siguientes acciones:

- Implementar las mejoras identificadas en el MSPI.
- Emprender las acciones correctivas y preventivas pertinentes para mejorar el MSPI.
- Comunicar las acciones de mejora a todas las partes interesadas.
- Asegurar que las mejoras logran los objetivos propuestos.

6. PLAN DE ACCIÓN PARA LA REALIZACIÓN E IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

POLÍTICA MIPG	PLAN INSTITUCIONAL	COMPONENTE	ACTIVIDADES	INDICADOR	META	AÑOS DE EJECUCIÓN			
						2019	2020	2021	2022
TIC para la	Plan de Seguridad y	PLANEAR	Definición del alcance del MSPI Definición del Gobierno de la SPI. Diseño de la Política general de la SPI. Diseño y presentación de las políticas específicas de SPI, en cuanto a, la organización de la SI uso de dispositivos móviles, SI en proyectos	Modelo de Seguridad y Privacidad de la Información Aprobado	1	5%	80%	80%	80%

Gestión y la SI	Privacidad de la Información.		Diseño y presentación de las políticas específicas de Seguridad en los recursos humanos, en cuanto a, la gestión de activos de información, acceso y uso de la información, clasificación de la información, Uso y protección de equipo de cómputo y redes de datos, uso del correo electrónico, impresoras, escritorio y pantallas limpias y al uso del Internet.	Políticas de Seguridad y Privacidad de la Información aprobadas.	1	5%	80%	80%	80%

POLÍTICA MIPG	PLAN INSTITUCIONAL	COMPONENTE	ACTIVIDADES	INDICADOR	META	AÑOS DE EJECUCIÓN			
						2019	2020	2021	2022
			Diseño y Presentación de la Política de seguridad física y ambiental, la de gestión de control de accesos, la de gestión de operaciones y comunicaciones, la de adquisición, desarrollo y mantenimiento de sistemas de información, la de gestión de incidentes de seguridad, la de gestión de proveedores, la de gestión de la continuidad del negocio y la de gestión y cumplimiento.					
			Determinación del compromiso de la alta dirección.	Asignación presupuestal para el sostenimiento del MSPI	1	5%	80%	80%	80%
			Definición de los Roles y Responsabilidades de la SPI.	Roles y responsabilidades	1	5%	80%	80%	80%

				aprobadas y asignadas					
			Elaborar y Presentar el Plan de Comunicaciones del MSPI.	Plan de Comunicaciones del MSPI aprobado	1	5%	80%	80%	80%
			Aprobación de la política de la SPI, con su alcance, objetivos, gobierno.	Políticas de Seguridad y Privacidad de la Información aprobadas.	1	5%	80%	80%	80%

POLÍTICA MIPG	PLAN INSTITUCIONAL	COMPONENTE	ACTIVIDADES	INDICADOR	META	AÑOS DE EJECUCIÓN			
						2019	2020	2021	2022
		HACER	La Formulación de un plan para el tratamiento de los Riesgos.	Plan para el Tratamiento de los Riesgos de TI	1	0%	80%	80%	80%
			Definición de controles para mitigar los riesgos.						
			Valoración de la eficacia de los controles definidos.						
			Realización de Programas de Formación.						
			Gestión de la Operación y los recursos del MSPI.						
			Implementación de las políticas y procedimientos definidos para la Seguridad y Privacidad de la Información.	(Número de procedimientos y políticas implementados/Número total de procedimientos y políticas a implementar) *100	100%	0%	100%	100%	100%

		VERIFICAR	Ejecución de los Procedimientos de seguimiento, revisión y otros controles para la SPI.	Procedimientos de seguimiento, revisión y controles ejecutados	100%	0%	80%	80%	80%
			Realización de revisiones a los controles, producto de las auditorias de SPI y la						

POLÍTICA MIPG	PLAN INSTITUCIONAL	COMPONENTE	ACTIVIDADES	INDICADOR	META	AÑOS DE EJECUCIÓN			
						2019	2020	2021	2022
			retroalimentación de las partes interesadas.	(Número de Auditorías realizadas al MSPI/Cantidad de Auditorias Programadas)	80%	0%	80%	80%	80%
			Realización de las auditorías internas al MSPI.						
			Medición de la eficacia de los Controles, para verificar que se cumplan los requisitos del MSPI.						
			Identificación y revisión de la valoración de los riesgos y amenazas.						
			Actualización de los planes de Seguridad y Privacidad de la Información.						
			Implementación de las mejoras identificadas en el MSPI.						

		ACTUAR	Cumplimiento y Realización de las acciones correctivas y preventivas pertinentes para mejorar el MSPI. Comunicación de las acciones de mejora a todas las partes interesadas.	(Número de Acciones de mejoramiento realizadas/Total de acciones de mejoramiento del proceso) *100	100%	0%	100%	100%	100%

POLÍTICA MIPG	PLAN INSTITUCIONAL	COMPONENTE	ACTIVIDADES	INDICADOR	META	AÑOS DE EJECUCIÓN			
						2019	2020	2021	2022
			Validación de las mejoras, para evidenciar que se logran los objetivos propuestos.						