PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI)

2020

Tecnológico de Antioquia Institución Universitaria

Contenido

1. OBJETIVO

Construir el plan de seguridad y privacidad de la información acorde a la misión y estrategia del Tecnológico de Antioquia acogiendo el Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL del Ministerio de Tecnologías de la Información y las Comunicaciones (Min-TIC), para estar acorde con las buenas prácticas de seguridad y teniendo en cuenta las normas ISO 27001 del 2013, Transparencia y Acceso a la Información Pública (Ley 1712 de 2014), la ley de Protección de Datos Personales, entre otras. Este modelo busca preservar la confiabilidad, disponibilidad e integridad de la información, generando estrategias para garantizar la privacidad y el buen uso de los datos que genera y posee la Institución dentro de sus sistemas de información.

2. ALCANCE DEL DOCUMENTO

Este documento busca identificar la metodología, los documentos y procesos que permitan desarrollar el PSPI de la Institución, definiendo las tareas generales en cada una de las etapas de implementación.

De esta forma la institución puede comenzar a definir, implementar y documentar el PSPI de una forma ordenada y de acuerdo a una metodología establecida que garantice el logro de los objetivos establecidos dentro del PSPI.

3. RECURSOS

Aquí se definen los recursos tanto humanos, físicos y financieros que soportan la implementación del PSPI.

Humanos: La definición e implementación del PSPI será liderado por el coordinador de las TIC del TdeA, apoyado por los profesionales que lideran los procesos de los diferentes Sistemas de información, Seguridad de la Información, Telecomunicaciones, Soporte, Infraestructura y acompañados por la oficina de gestión de calidad de la institución.

Físicos: Para lograr los objetivos trazados dentro de la implementación del PSPI se hace necesario el acceso a los equipos de control perimetral con que cuenta la Institución (Firewall, IDS/IPS), al equipo de análisis de tráfico que permitirá una visión más real de lo que está pasando en el perímetro de la red de datos, además el acceso a los centros de cableado, switches CORE y de borde.

4. FASES DE IMPLEMENTACIÓN

Acogiendo lo planteado en el modelo de seguridad y privacidad de la información del MinTIC (MSPI), donde se plantean cinco (5) fases que sirven de ruta para el desarrollo de dicho modelo y permite gestionar de una forma adecuada la seguridad y la privacidad de la información como componente fundamental de los procesos institucionales, se definen las siguientes fases:

Diagnóstico: En esta fase se realiza un levantamiento de información que pretende identificar el estado actual de la seguridad y la privacidad de la información e identificar su nivel de madurez.

Planificación: Partiendo de los resultados de la fase de diagnóstico, se procede a la elaboración del PSPI alineado con el objetivo misional Institucional, definiendo las acciones a implementar y los alcances de dicho plan.

Implementación: Se implementan todas las acciones planteadas en la fase de planificación, teniendo en cuenta indicadores de gestión y tratamiento de la seguridad y privacidad de la información.

Evaluación de Desempeño: A través de auditorías internas, monitoreo, medición y evaluación de controles y los resultados que arrojan los indicadores de la seguridad de la información se puede verificar la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Mejora continua: En esta fase se define el plan de mejoramiento continuo donde se toman acciones para mitigar las debilidades encontradas, de acuerdo a los resultados obtenidos en la fase de evaluación de desempeño.

5. CRONOGRAMA

Fase	Meta	Resultado	Fecha
Diagnostico	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Febrero 2020
	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Febrero 2020
	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Marzo 2020

Fase	Meta	Resultado	
Planificación	Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales	Mayo 2020
	Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Junio 2020
	Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Junio 2020
	Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Junio 2020
	Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Septiembre 2020
	Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad	Septiembre 2020
	Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	Octubre 2020

Fase	Meta	Resultado	Fecha
Implementación	Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Diciembre 2020

Fase	Meta	Resultado	Fecha
Evaluación de desempeño	Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Diciembre 2020

Fase	Meta	Resultado	Fecha
Mejora Continua	Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Diciembre 2020

6. SEGUIMIENTO Y EVALUACIÓN

Como se establece en el cronograma todas las fases requieren un seguimiento, unas metas y evaluación que permiten definir las mejores prácticas en cada caso concreto. En reuniones periódicas con el grupo primario que lidera el coordinador de las TIC de la Institución, se socializan todas las actividades y eventos que afectan el PSPI y se hace entrega de documentos o avances asignados en cada fase. De todas estas reuniones se elaboran actas.