PLAN ANUAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2020

TECNOLOGÍAS Y SISTEMAS DE LA INFORMACIÓN

Soledad Atlántico, 2020

INTRODUCCIÓN

La Institución Universitaria ITSA, comprometida con el fortalecimiento de la protección y aseguramiento de su información, continua durante la vigencia 2020, con la implementación del modelo de seguridad y privacidad de la información MSPI con base en un diagnóstico previo de la situación actual, la identificación de vulnerabilidades, formalización de políticas e identificación de los activos de información, entre otros. Para esta vigencia se han establecido unas metas relacionadas con la gestión de las vulnerabilidades identificadas, gestión de riesgos de seguridad digital, plan de comunicaciones relacionadas con seguridad de la información, diagnóstico de IPv4 a IPv6 y Planificación y Control Operacional.

OBJETIVO

Establecer y priorizar las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la información MSPI y que se ejecutarán en la vigencia 2020, alineadas con el marco normativo de la ISO 27001 y la política de Gobierno Digital.

ALCANCE

El alcance del presente plan anual comprende la ejecución de acciones pendientes al cumplimiento de los requisitos y componentes definidos para la implementación del Modelo de Seguridad y Privacidad de la Información y la Norma ISO 27001, para la vigencia 2020.

CONTENIDO DEL PLAN

De acuerdo a la normatividad vigente y la norma ISO 27001, orientada al aseguramiento, la confidencialidad e integridad de la información, la Institución Universitaria ITSA establece el siguiente plan para esta vigencia, estableciendo una serie de metas y actividades pendientes a ejecutar, alineadas con los objetivos y metas institucionales, continuando así con el proceso de implementación del Modelo de Seguridad y Privacidad de la Información, basado en el diagnóstico previo realizado sobre el nivel de madurez que posee la institución relacionado con la gestión de la seguridad y privacidad de la información.

Para la vigencia 2020, este plan comprende las siguientes metas:

- **Gestionar las vulnerabilidades de nivel alto y crítico de los hallazgos encontrados en las pruebas de vulnerabilidad.**
- **Identificar, valorar y tratar los riesgos.**
- **Elaborar Plan de comunicaciones.**
- **Actualizar Plan de diagnóstico IPv4 a IPv6.**
- **Elaborar Planificación y Control Operacional.**

La siguiente tabla muestra las actividades del Plan Anual del Modelo de Seguridad y privacidad de la información para la vigencia 2020.

ACTIVIDADES PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

METAS	ACTIVIDADES	PRODUCTO
Gestionar las vulnerabilidades de nivel alto y crítico de los hallazgos encontrados en las pruebas de vulnerabilidad	* Analizar las vulnerabilidades críticas identificadas. * Aplicar parches de seguridad y/o ajustes necesarios para eliminar las vulnerabilidades críticas identificadas.	Documento con las evidencias de las vulnerabilidades gestionadas de nivel alto y crítico en 5 servidores.
Identificar, valorar y tratar los riesgos	Identificar los riesgos de seguridad digital.	Documento con mapa de riesgos de seguridad digital.
Elaborar plan de comunicaciones	* Elaboración del plan de comunicación, sensibilización y capacitación referente a seguridad digital * Cumplir con el 80% de las actividades contenidas en el plan.	Documento con el Plan de comunicación, sensibilización y capacitación para la entidad sobre seguridad de la información.
Actualizar plan de diagnóstico IPv4 a IPv6	Realizar actualización del documento sobre el plan de diagnóstico para la transición de IPv4 a IPv6.	Documento actualizado con el plan de diagnóstico para la transición de IPv4 a IPv6.
Elaborar planificación y control operacional	Realizar documento sobre declaración de aplicabilidad relacionado con controles de seguridad de la información.	Documento con declaración de aplicabilidad.

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

METAS	2020									
	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Gestionar las vulnerabilidades de nivel alto y crítico de los hallazgos encontrados en las pruebas de vulnerabilidad										
Analizar las vulnerabilidades críticas identificadas										
Aplicar parches de seguridad y/o ajustes necesarios para eliminar las vulnerabilidades críticas identificadas.										
Identificar, valorar y tratar los riesgos										
Identificar los riesgos de seguridad digital										
Elaborar plan de comunicaciones										
Elaboración del plan de comunicación, sensibilización y capacitación referente a seguridad digital										
Cumplir con el 80% de las actividades contenidas en el plan										
Actualizar plan de diagnóstico IPv4 a IPv6										
Realizar actualización del documento sobre el plan de diagnóstico para la transición de IPv4 a IPv6										
Elaborar planificación y control operacional										
Realizar documento sobre declaración de aplicabilidad relacionado con controles de seguridad de la información.										