DIVISIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI
UNIVERSIDAD DEL CAUCA

Preparado	Jorge A. Martínez G.
Revisado	Oscar J. Calderón C.
Versión	1.0
Tipo	Documento de trabajo

Universidad del Cauca
Popayán, diciembre 2019

Contenido

Introducción 3
Objetivos 3
Objetivo General: 3
Objetivos específicos: 3
Generalidades 4
Contexto estratégico 4
Alcance 4
Contexto normativo 4
Definiciones: 4
Desarrollo del plan seguridad y privacidad de la información 5
Metodología de implementación 5
Etapas previas a la implementación: 6
Implementación: 7
Estado actual: 7
Trabajo a seguir: 7

Introducción

La universidad del Cauca, mediante el presente documento establece el borrador del Plan de Seguridad y Privacidad de la Información, definiendo un conjunto de actividades basadas en el ciclo PHVA (Planificar-Hacer- Verificar-Actuar) para establecer un uso adecuado de la información, mediante un enfoque basado en la gestión de riesgos, con el objetivo de brindar niveles adecuados de confidencialidad, integridad y disponibilidad de la información de la Institución, basado principalmente en la Norma Técnica Colombiana ISO27001:2013.

Este documento establece los objetivos, generalidades, contexto, alcance, contexto normativo, definiciones, metodología de implementación y etapas para el Plan de Seguridad y Privacidad de la Información.

Objetivos

Objetivo General:

Mantener la integridad, confidencialidad y disponibilidad de la información perteneciente a los sistemas críticos de la universidad del Cauca brindados por la división de tecnologías de la información y las comunicaciones.

Objetivos específicos:

1.Actualizar los activos de información de la División de Tecnologías de la universidad del Cauca y su criticidad en relación a la integridad, confidencialidad y disponibilidad de la información.

2.Identificar los riesgos en los procesos de la División de Tecnologías de la universidad del Cauca, que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

3.Atender de manera adecuada los incidentes de seguridad de la información que afecte la integridad, confidencialidad y disponibilidad de la misma.

4.Cumplir la normatividad legal vigente incluyendo la norma ISO 27001:2013, la Ley estatutaria de protección de datos personales (Ley 1581 de 2012) y sus decretos reglamentarios y las normas que las modifiquen, adicionen o sustituyan.

5.Realizar campaña de cultura y concientización en seguridad y privacidad de la información para los funcionarios, docentes y contratistas de la universidad del Cauca.

Generalidades

Contexto estratégico

El presente plan está alineado con las directrices universitarias y con el plan estratégico de la institución.

Alcance

El presente plan aplica al subproceso de recursos tecnológicos y sus procedimientos relacionados. Considerando la posible extrapolación a otras dependencias donde tenga lugar la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

Contexto normativo

Se toman como base y referencias las normas aplicables en el área de seguridad de la información incluyendo:

Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

Guia de MinTIC G.ES.05 Diseño e implementación de una estrategia de seguridad de la información.

Norma Técnica Colombiana ISO27001:2013.

Norma Técnica Colombiana ISO31000:2013.

Resolución interna, Resolución R-785 de 2015 (política del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca).

Definiciones:

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Integridad: propiedad de exactitud y completitud.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Incidente de seguridad de la información: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando la confidencialidad, integridad o disponibilidad de la información.

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales. Se expresa en términos de probabilidad y consecuencias.

Desarrollo del plan seguridad y privacidad de la información

Metodología de implementación

La metodología de implementación del Plan de Seguridad y Privacidad para la Universidad del Cauca, está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, tal como se ilustra en la figura 1:

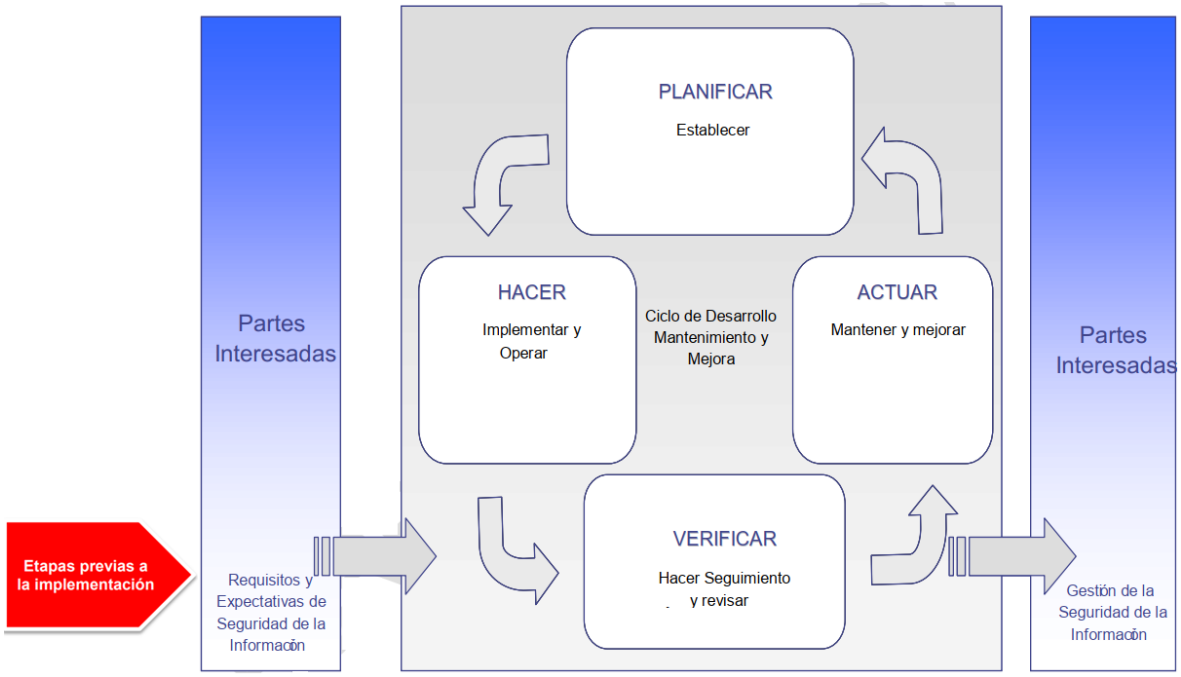

Figura 1. Ciclo PHVA para planes de seguridad de la información. (Adaptado por el autor)

Las etapas definidas incluyen:

Etapas previas a la implementación:

Estado actual de la entidad
Levantamiento de información Planificación:
Contexto de la entidad.
Liderazgo
Planeación

Como parte de la etapa previa a la implantación, se establece el seguimiento de los pasos planteados en la guía MINTIC de estrategia de seguridad, iniciando con la identificación del estado actual y finalizando con la definición y ejecución del plan. Figura 2.

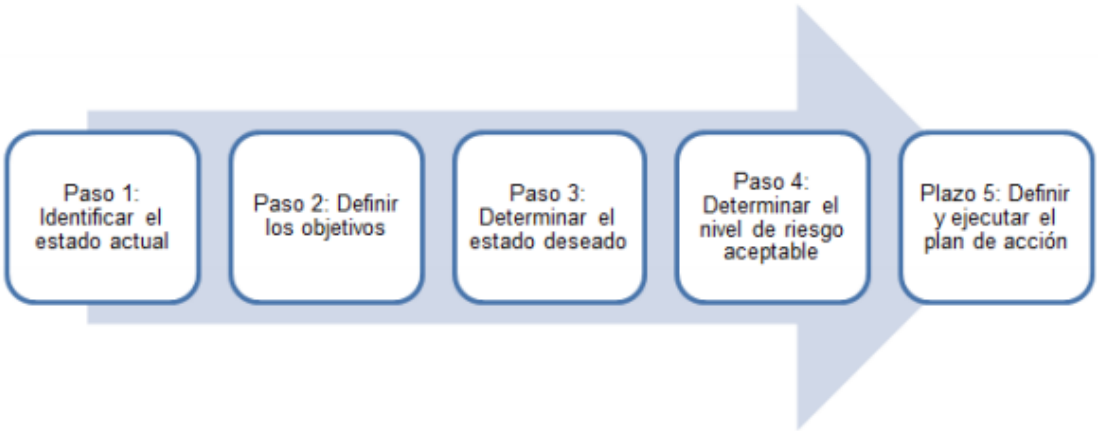

Figura 1. Etapas previas para implementación del plan de seguridad

Implementación:

Control y planeación operacional
Evaluación de riesgos de Seguridad y Privacidad de la Información
Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
Evaluación de Desempeño:
Monitoreo, medición, análisis y evaluación.
Auditoria interna Mejora continua:
Acciones correctivas y no conformidades

Estado actual: etapa previa a implementación.

Se tiene definida la política de seguridad mediante resolución R-785 de 2015 (política del Sistema de Gestión de Seguridad de la Información de la Universidad del Cauca).

Se tiene formulado el proyecto SGSI.

Se tiene procedimiento de seguridad División TIC publicado en programa lvmen.

Trabajo a seguir:

Establecimiento de políticas División TIC.
Evaluación de estado actual basado en MSPI.
Levantamiento de información

El desarrollo del proyecto e implementación del SGSI debe contar con el apoyo financiero y compromiso humano para que sea coherente con las normas internas y requerimientos nacionales, como apoyo al mejoramiento de los procesos institucionales seguros y confiables.