UNIDAD CENTRAL DEL VALLE DEL CAUCA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1.0

Historial de Revisiones

Fecha	Versión	Descripción	Autor
23/06/2018	1.0	Creación del documento	Maritza Beltrán García

CONTENIDO

ILUSTRACIONES

TABLAS

INTRODUCCIÓN

La Unidad Central del Valle del Cauca, UCEVA, es una Institución Universitaria Pública de Educación Superior, creada mediante el Acuerdo No. 24 de junio de 1971, del Honorable Concejo Municipal de Tuluá - Valle del Cauca, como alternativa de acceso a la educación superior para los bachilleres del centro y norte del Valle del Cauca.

Se realiza el presente documento con el propósito de dar a conocer el proceso de implementación y socialización del Sistema de Gestión de Seguridad y Privacidad de la Información SGSPI, alineado con la política de Gobierno Digital y el modelo integrado de planeación y gestión – MIPG y las disposiciones de la ley 1581 de 2012, decreto 1377 de 2013 y el decreto 886 de 2014.

1 ALCANCE

Se identifica la metodología, documentos y procesos que permitirán a la institución desarrollar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PRSI, precisando las fases proyecto de implementación y sus tareas macro; garantizando de esta forma un trabajo estructura para la minimización de riesgos informáticos asociados a la seguridad y privacidad de la información.

2 OBJETIVO

Identificar, controlar y minimizar los riesgos informáticos asociados a la seguridad y privacidad de la información de los procesos institucionales existentes, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios, asegurando la confidencialidad, integridad y privacidad de la información.

.

2.1 Objetivos específicos

- Definir la metodología, fases y actividades para la implementación del PRSI.
- Elaborar un plan de trabajo para la implementación de PRSI.
- Identificar los riesgos actuales, las posibles causas y sus controles.

3 RECURSOS

Humanos

La definición e implementación del PRSI será liderado por el Jefe de la Oficina de Informática y Telemática, apoyado por su equipo de trabajo, así como de la Oficina Asesora de Planeación y la Oficina de Control Interno.

Físicos

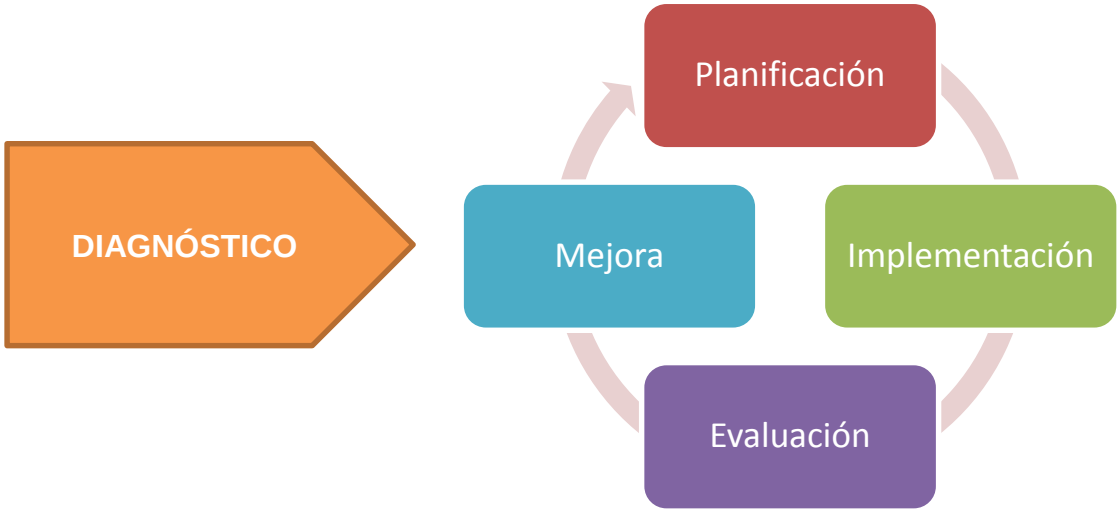
Para lograr los objetivos trazados dentro de la implementación del PRSI se hace necesario el acceso a los equipos de seguridad perimetral con que cuenta la Institución (Firewall, IDS/IPS), así como contar con un equipo de análisis de tráfico que permita tener una visión real de lo que está pasando en el perímetro de la red de datos. Acceso a los centros de cableado, switches CORE y de borde. En conclusión, se necesita acceso a la infraestructura tecnológica, controles de acceso físico.

4 METODOLOGÍA DE IMPLEMENTACIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), organismo encargado de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones, ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información – MSPI, acorde con las buenas prácticas de seguridad, y alineado con el Marco de Referencia de Arquitectura TI.

A nivel metodológico el MSPI de MinTIC, incluye una serie de guías en cada una de las fases del modelo, por lo tanto, a nivel institucional se adopta dicho modelo y la metodología incluida; alineadas con la metodología PHVA (Planear, Hacer, Verificar y Actuar), y el modelo integrado de planeación y gestión – MIPG.

lustración 1 Metodología de MSPI



Fuente: MinTIC. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

5 FASES DE IMPLEMENTACIÓN

5.1 Diagnóstico

Fase preliminar. Se identifica el estado actual de la institución con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información a través del diagnóstico de:

1. Estado actual de la institución
2. Identificación del nivel de madurez
3. Levantamiento de información

Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

5.2 Planificación

A partir del diagnóstico, se definen las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo. Se definen, para todos los procesos institucionales, los límites de la implementación basados en el alcance.

1. Contexto de la institución
    a. Entender la institución
    b. Necesidades y expectativas de las partes interesadas
    c. Determinar alcance del MSPI
2. Liderazgo
    a. Liderazgo y compromiso de la alta dirección
    b. Política de seguridad
    c. Roles de la institución, responsabilidades y autoridad

3. Planeación
    a. Acciones para abordar los riesgos y oportunidades
    b. Objetivos y planes para lograrlos
4. Soporte
    a. Recursos
    b. Competencias
    c. Sensibilización
    d. Comunicación
    e. Documentación

5.3 Implementación

En esta fase se lleva a cabo la implementación de la planeación realizada en la fase anterior, y está compuesta por:

1. Control y planeación operacional
2. Plan de Tratamiento de riesgos de seguridad y privacidad de la información
3. Definición de Indicadores de Gestión

5.4 Evaluación

La evaluación se realiza en términos de efectividad, la eficiencia y la eficacia de las acciones implementadas, con base en los resultados de los indicadores definidos, a través de las siguientes actividades:

1. Monitoreo, medición, análisis y evaluación
2. Auditoría interna
3. Revisión por la alta dirección

5.5 Mejora Continua

La mejora continua se logra a través de la consolidación de los resultados de la evaluación, diseñando un plan de mejoramiento que permita mitigar las debilidades identificadas. La mejora continua se basa en las actividades:

1. Acciones correctivas
2. Oportunidades de mejora

Al finalizar cada fase se debe realizar una reunión con la alta dirección de la Institución para presentar el informe del avance del proyecto, (resumen ejecutivo), y evaluar posibles ajustes al mismo.

6 CRONOGRAMA

Fase	Meta	Entregable	Fecha
DIAGNÓSTICO	Determinar el estado actual de la gestión de seguridad y privacidad de la información	Herramienta de diagnóstico diligenciada	Oct-18
	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Herramienta de identificación de madurez diligenciada	Nov-18
	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad	Dic-18
PLANEACIÓN	Política de Seguridad y Privacidad de la Información	Política aprobada por la alta y socializada.	Feb-19
		Manual con las políticas de seguridad y privacidad de la información aprobadas y socializadas	Mar-19
	Procedimientos de seguridad de la información	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Abr-19
	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.	May-19
	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 Inventario de activos de IPv6	Jul-19
	Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Ago-19
	Identificación, Valoración y tratamiento	Documento con la metodología de	Oct-19

Fase	Meta	Entregable	Fecha
	de riesgo.	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.	
	Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Nov-19
	Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Dic-19
IMPLEMENTACIÓN	Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Feb-20
	Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Mar-20
	Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Abr-20
	Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	May-20
EVALUACIÓN	Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Jun-20
	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.	Jul-20
MEJORA	Plan de mejora continua	Documento con el plan de mejoramiento.	Jul-20
		Documento con el plan de comunicación de resultados.	Ago-20