Institución de Educación Superior
UCEVA
Unidad Central del Valle del Cauca

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

OFICINA DE INFORMÁTICA Y TELEMÁTICA

Historial de Revisiones

Fecha	Versión	Descripción	Autor
22/06/2018	1.0	Creación del documento	Maritza Beltrán García
03/07/2019	1.1	Actualización	Maritza Beltrán García
05/03/2020	1.2	Actualización	Juan Carlos Tascón Restrepo
14/01/2021	1.3	Actualización	Juan Carlos Tascón Restrepo
19/11/2021	1.4	Actualización	Juan Carlos Tascón Restrepo

CONTENIDO

ILUSTRACIONES

TABLAS

INTRODUCCIÓN

El plan de seguridad y privacidad de la información (PSPI) contribuyen a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la Institución apoyada en el uso adecuado de las TIC.

la Unidad Central del Valle del Cauca - UCEVA debe contar con un proceso de seguridad que garantice la efectividad de los controles definidos para la custodia de los activos, que vele porque la información sea correcta y sea completa, esté siempre a disposición del cumplimiento de las metas de la institución y esté respaldada y sea utilizada sólo por aquellos que tienen autorización para hacerlo. (PSPI, 2020).

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas. (MINTIC, 2016).

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Unidad Central del Valle del Cauca - UCEVA, está determinada por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad. (MINTIC, 2016).

Se efectúa el actual documento con la intención de colocar en conocimiento a el proceso de implementación y socialización del Sistema de Gestión de Seguridad y Privacidad de la Información SGSPI, articulado 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. (PSPI, 2020).

1 OBJETIVO

El Objetivo primordial del Plan de implementación para el Modelo de Seguridad y Privacidad de la Información, es precisar las acciones a tomar por la Unidad Central del Valle del Cauca - UCEVA para preservar la integridad, confidencialidad y disponibilidad de la información; las prioridades de ejecución, los recursos necesarios para llevarlas a cabo y el seguimiento para verificar la eficacia del mismo, Implementando lineamientos de buenas prácticas en Seguridad y Privacidad de la Información. (PSPI, 2020).

1.1 OBJETIVOS ESPECÍFICOS

- Contribuir al incremento de la transparencia en la gestión pública.
- Definir la metodología, fases y actividades para la implementación del PSPI.
- Elaborar un plan de trabajo para la implementación de PSPI.
- Contribuir en el desarrollo del plan estratégico institucional y del PETI.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de ciberseguridad en la entidad.
- Alinear el marco de referencia de arquitectura empresarial con los principios de seguridad y privacidad de la información.

2 ALCANCE

Se identifica la metodología, documentos y procesos que permitirán a la institución desarrollar el Plan de Seguridad y Privacidad de la Información – PSPI, precisando las fases de su implementación y sus tareas macro; garantizando de esta forma el tratamiento de la información utilizada en los trámites y servicios que ofrece la Institución, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

3 RECURSOS

3.1 Humanos

La definición e implementación del PSPI 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. (PSPI, 2020).

3.2 Físicos

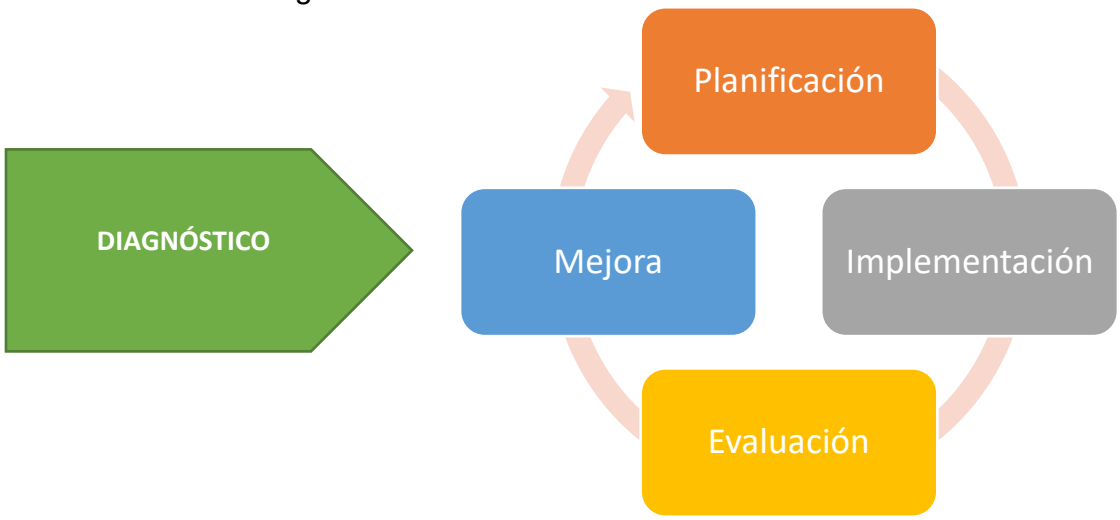
Para lograr los objetivos trazados dentro de la implementación del PSPI se hace necesario el acceso a los equipos de seguridad perimetral con que cuenta la Institución (Firewall, IDS/IPS), así como contar con un equipo de análisis de tráfico que permita tener una visión real de lo que está pasando en 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. (PSPI, 2020).

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. (MINTIC, 2016).

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. (MINTIC, 2016).

lustración 1 Metodología de MSPI



Fuente: MinTIC. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información MINTIC (2016).

5 FASES DE IMPLEMENTACIÓN

5.1 Fase 1: componente – diagnóstico.

Fase preliminar. De acuerdo con PSPI (2020), 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:

- Estado actual de la institución
- Identificación del nivel de madurez
- 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 Fase 2: componente – planificación PSPI (2020).

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.

- Contexto de la institución
  - Entender la institución
  - Necesidades y expectativas de las partes interesadas
  - Determinar alcance del MSPI

- Liderazgo
  - Liderazgo y compromiso de la alta dirección
  - Política de seguridad
  - Roles de la institución, responsabilidades y autoridad
- Planeación
  - Acciones para abordar los riesgos y oportunidades
  - Objetivos y planes para lograrlos

- Soporte
  - Recursos
  - Competencias
  - Sensibilización
  - Comunicación
  - Documentación

5.3 Fase 3: componente – implementación PSPI (2020).

La ejecución de esta etapa permitirá a la Institución la implementación de los aspectos identificados en las fases anteriores (diagnóstico y planeación) y está compuesta por:

- Control y planeación operacional
- Plan de Tratamiento de riesgos de seguridad y privacidad de la información
- Definición de Indicadores de Gestión

5.4 Fase 4: componente – evaluación PSPI (2020).

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:

- Monitoreo, medición, análisis y evaluación
- Auditoría interna
- Revisión por la alta dirección

5.5 Fase 5: componente - mejora continua PSPI (2020).

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:

- Acciones correctivas
- 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	% Ejecución
DIAGNÓSTICO	Determinar el estado actual de la gestión de seguridad y privacidad de la información	Herramienta de diagnóstico diligenciada	Ago-2020	100
	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Herramienta de identificación de madurez diligenciada	Sep-2020	100
	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad	Oct-2020	100
PLANEACIÓN	Política de Seguridad y Privacidad de la Información	Política aprobada por la alta y socializada.	Nov-2020	100
		Manual con las políticas de seguridad y privacidad de la información aprobadas y socializadas	Dic-2020	100
	Procedimientos de seguridad de la información (Plan de Calidad)	Procedimientos (planes de calidad), debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Feb-2022	50
	Roles y responsabilidades de seguridad y privacidad de la información.	Resolución rectoral a través del cual se definen las instancias al interior de la institución que se encargarán de revisar, de velar el Cumplimiento y el mejoramiento continuo de la política de Seguridad y privacidad de la información de la unidad central del valle del cauca, revisada y aprobada por la alta Dirección.	Dic-2021	100
	Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado, revisado y aprobado por el CIGED.	Feb-2022	90
		Matriz con la identificación, valoración y clasificación de activos de información.	Junio-2022	15

Fase	Meta	Entregable	Fecha	% Ejecución
		Documento con la caracterización de activos de información, que contengan datos personales	Junio-2022	5
		Inventario de activos de IPv6	Diciembre -2021	100
	Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Dic-2022	10
	Identificación, Valoración y tratamiento de riesgo.	• Documento Matriz con la metodología de gestión de riesgos, análisis y evaluación de riesgos, plan de tratamiento de riesgos. • Documento con la declaración de aplicabilidad. • Documentos revisados y aprobados por la alta Dirección.	Marzo-2022	70
	Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Dic-2021	100
	Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Nov-2022	27
IMPLEMENTACIÓN	Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Abril-2022	0
	Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Dic-2022	0
	Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Jun-2022	50
	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.	Oct-2022	0
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.	Oct-2022	0
	Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al	Oct-2022	0

Fase	Meta	Entregable	Fecha	% Ejecución
		MSPI, revisado y aprobado por la Alta Dirección.		
MEJORA	Plan de mejora continua	Documento con el plan de mejoramiento.	Dic-2022	0
		Documento con el plan de comunicación de resultados.	Dic-2022	0

7 SEGUIMIENTO

Para efectos de seguimiento al presente Plan de Seguridad y Privacidad de la Información 2022, se hará uso de la siguiente matriz, que además fue incorporada al Plan de Acción Institucional de la misma vigencia, como mecanismo de articulación y efectividad en el direccionamiento estratégico de la UCEVA.

Tabla 1 Matriz de Seguimiento y Articulación con Plan de Acción Institucional 2022

Caracterización						*Medición*			
Etapa	**No.**	**Actividad a realizar**	**¿Requiere presupuesto?**	**Si requiere presupuesto, especifique de qué tipo (Funcionamiento / Proyecto de Inversión)**	**Si seleccionó de inversión ¿A que proyecto de inversión está asociado?**	**Meta**	**Indicadores**	**Temporalidad de medición**	**Observaciones**
Planeación	1	Culminar los Procedimientos (planes de calidad), debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	NO			9	Cantidad de Planes Realizados / Cantidad de Planes Planeados * 100	ANUAL	
	2	Generar documento con la metodología para identificación, clasificación y valoración de activos de información, validado, revisado y aprobado por el CIGED.	NO			1	Documento	ANUAL	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado, revisado y aprobado por el CIGED.
	3	Realizar Matriz con la identificación, valoración y clasificación de activos de información.	NO			1	Matriz	ANUAL	
	4	Generar Documento con la caracterización de activos de información, que contengan datos personales	NO			1	Documento	ANUAL	
	5	Realizar la Integración del MSPI, con el sistema de gestión documental de la entidad.	NO			1	Proceso de integración	ANUAL	Se debe adquirir software especializado para cumplir con las normas establecidas por Mintic
	6	Elaborar los siguientes Documentos : Documento Matriz con la metodología de gestión de riesgos, análisis y evaluación de riesgos, plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	NO			3	Documentos	ANUAL	
	7	Generar el documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	SI	INVERSIÓN	Consolidación del ecosistema digital, articulado a la alta calidad institucional y el mejoramiento continuo de la Unidad Central del Valle del Cauca	1	Documento	ANUAL	

Caracterización						Medición			
Etapa	**No.**	**Actividad a realizar**	**¿Requiere presupuesto?**	**Si requiere presupuesto, especifique de qué tipo (Funcionamiento / Proyecto de Inversión)**	**Si seleccionó de inversión ¿A que proyecto de inversión está asociado?**	**Meta**	**Indicadores**	**Temporalidad de medición**	**Observaciones**
Implementación	**8**	Elaborar Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	NO			1	Documento	ANUAL	
	9	Realizar Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	NO			1	Informe	ANUAL	
	10	Hacer documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	NO			1	Documento	ANUAL	
	11	Elaborar el Plan de Transición de IPv4 a IPv6	SI	INVERSIÓN	Consolidación del ecosistema digital, articulado a la alta calidad institucional y el mejoramiento continuo de la Unidad Central del Valle del Cauca	1	Documento	ANUAL	
Evaluación	**12**	Construcción del Plan de revisión y seguimiento, a la implementación del MSPI	NO			1	Plan	ANUAL	
	13	Construcción del Plan de Ejecución de Auditorias	NO			1	Plan	ANUAL	
Mejora	**14**	Construcción del Plan de mejora continua	NO			1	Plan	ANUAL	