Institución de Educación Superior
UCEVA
Unidad Central del Valle del Cauca

Plan de Seguridad y Privacidad de la Información

2023

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
02/12/2022	1.5	Actualización	Paola Andrea Mosquera palacios

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).

MARCO NORMATIVO

El marco normativo o jurídico en el cual se fundamenta el Plan de Seguridad y Privacidad de la Información, para la Unidad Central del Valle del Cauca -UCEVA, es el siguiente:

Marco Normativo	Descripción
Decreto 1151 de 2008	“Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones”.
Ley 1955 del 2019	“Establece que las entidades del orden nacional deberán incluir en su plan de acción el compnente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)”.
Ley 1266 de 2008	"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".
Ley 1273 de 2009	“Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
Ley 1341 de 2009	“Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones”.
Ley 1581 de 2012	“Por la cual se dictan disposiciones generales para la protección de datos personales”.
Ley 1712 de 2014	“Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones”.
Ley 962 de 2005	El artículo 14 menciona lo siguiente: “Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá al usuario. Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. El envío de la información por fax o cualquier otro medio de transmisión electrónica, proveniente de una entidad pública, prestará mérito suficiente y servirá de prueba en la actuación de que se trate siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite”.
Ley 527 de 1999	"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
Ley 599 de 2000	"Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático".
Decreto 1413 de 2017	“En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales”.
Decreto 2620 de 1993	"Por medio del cual se reglamenta el procedimiento para la utilización de medios tecnológicos para conservar los archivos de los comerciantes".
Decreto 1524 de 2002	"Establecer las medidas técnicas y administrativas destinadas a prevenir el acceso a menores de edad a cualquier modalidad de información pornográfica contenida en Internet o en las

Marco Normativo	Descripción
	distintas clases de redes informáticas a las cuales se tenga acceso mediante redes globales de información".
Decreto 2150 de 1995	"Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública".
Decreto 4485 de 2009	"Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública".
Decreto 235 de 2010	"Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas".
Decreto 2364 de 2012	"Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones".
Decreto 2693 de 2012	"Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones".
Decreto 1377 de 2013	"Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales".
Decreto 4170 de 2011	"Mediante el cual se establece un sistema para la compra en entidades públicas, se determina que debe existir un Sistema de Información en el cual se almacene y se de trazabilidad a las etapas de contratación del país, garantizando la transparencia de los procesos".
Decreto 2693 de 2012	"Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones".
Decreto 2573 de 2014	"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".
Decreto 2433 de 2015	"Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
Decreto 1078 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
Decreto 103 de 2015	"Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
Decreto 415 de 2016	"Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones".
Decreto 728 2016	"Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico".
Decreto 728 de 2017	"Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico".
Decreto 1499 de 2017	"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".
Decreto 612 de 2018	"Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".

Marco Normativo	Descripción
Decreto 1008 de 2018	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
Decreto 2106 del 2109	"Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva".
Decreto 620 de 2020	"Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Decreto 767 de mayo 16 de 2022	"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
Resolución 2710 de 2017	"Por la cual se establecen los lineamientos para la adopción del protocolo IPv6".
Resolución 3564 de 2015	"Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública".
Resolución 3564 2015	"Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)".
Resolución 1519 de 2020	"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"
Norma Técnica Colombiana NTC 5854 de 2012	"Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA".
CONPES 3292 de 2004	"Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos".
CONPES 3920 de Big Data, del 17 de abril de 2018	"La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales".
CONPES 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016	"El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo".
CONPES 3975	"Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema".

Marco Normativo	Descripción
Circular 02 de 2019	“Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad”.
Directiva 02 2019	“Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones”.

Fuente: Normograma Institucional Uceva 2022

OBJETIVOS

2.1 OBJETIVO GENERAL

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).

2.2 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.

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.

Ilustración 1RECURSOS

4.1 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).

4.2 FÍSICOS

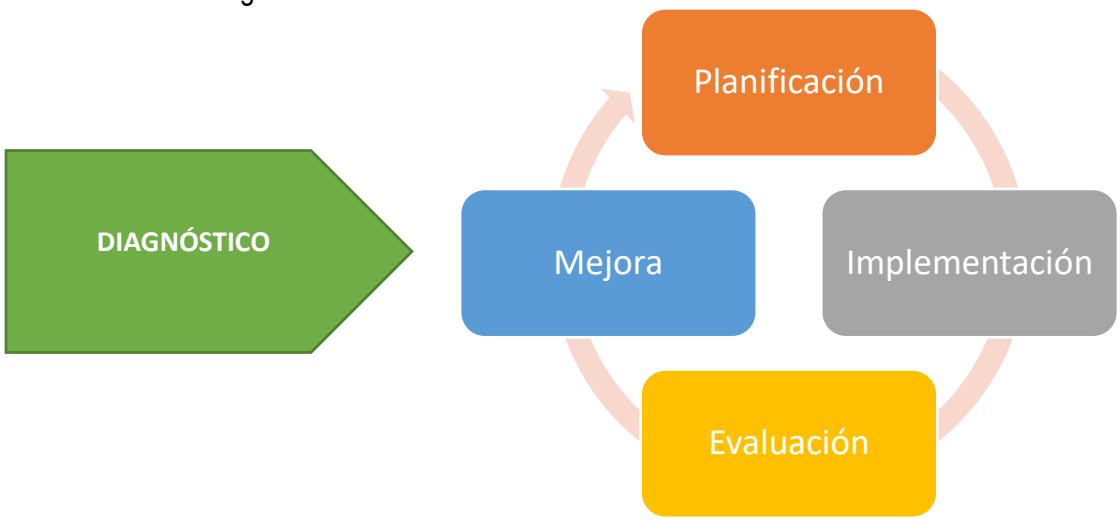
Para lograr los objetivos trazados dentro de la implementación del PSPI se hace necesario el acceso a los equipos de seguridad perimetral con que cuenta la Institución (Firewall, IDS/IPS), así como contar con un equipo de análisis de tráfico que permita tener una visión real de lo que está pasando en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

5 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 2 Metodología de MSPI



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

6 FASES DE IMPLEMENTACIÓN

6.1 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.

6.2 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

6.3 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

6.4 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

6.5 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.

7 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.	Dic-2022	100
	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	100
		Actualización de Matriz con la identificación, valoración y clasificación de activos de información.	Sept-2023	0
		Actualización del Documento con la caracterización de activos de información, que contengan datos personales	Sept-2023	0
		Actualización Inventario de activos de IPv6	Diciembre-2023	0
	Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Dic-2023	30
	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.	Dic-2023	70

Fase	Meta	Entregable	Fecha	% Ejecución
	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	100
IMPLEMENTACIÓN	Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Abril-2022	100
	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	100
	Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Jun-2022	100
	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	100
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	100
	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.	Oct-2023	0
MEJORA	Plan de mejora continua	Documento con el plan de mejoramiento.	Dic-2023	0
		Documento con el plan de comunicación de resultados.	Dic-2023	0

Tabla 1 Matriz de Ejecución Plan de Seguridad y Privacidad de la Información - PSPI 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	Se Realizaron 4 instructivos, 5 planes de calidad y 1 manual , para un total de 10 documentos que estan cargados en el aplicativo isolución
	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	Se encuentra el Plan de Calidad de inventario de activos **GDI-GSIN-D013**
	3	Realizar Matriz con la identificación, valoración y clasificación de activos de información.	NO			1	Matriz	ANUAL	Se evidencia en ISOLUCION la matriz de activos de información para el año 2022 "Inventario_Activos-_Informacion_Uceva 2022_Informatica" e "1045 Formato Inventario_Activos-_Informacion 2022 informacion"
	4	Generar Documento con la caracterización de activos de información, que contengan datos personales	NO			1	Documento	ANUAL	Se encuentra evidencia en ISOLUCION con el código **GDI-GSIN-F037,** Plan de Calidad de inventario de activos **GDI-GSIN-D013** y la matriz "Inventario_Activos-_Informacion_Uceva 2022_Informatica" e "1045 Formato Inventario_Activos-_Informacion 2022 informacion" con la caracterización de datos personales
	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 , pero se genero un Google Drive para el almacenamiento de información documental clasificada como electronica o digital segun la TRD de cada dependencia.
	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	En el aplicativo Isolución como un registro se encuentra "Matriz riesgos de seguridad digital Plantilla-v1-2022" , donde se puede evidenciar la metodología de gestión de riesgos, análisis y evaluación de riesgos y el plan de tratamiento de riesgos. queda Faltando el documento de declaración de aplicabilidad, revisado y aprobado por la alta dirección
	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	Se encuentra encuentra cargado en el aplicativo Isolución como un registro con el formato de MINTIC con el nombre Plan Diagnostico IPv6 UCEVA-2020
Implementación	8	Elaborar Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	NO			1	Documento	ANUAL	se generaron planes de calidad para los diferentes procesos relacionados con la seguridad y privacidad de la información. asimismo En la Matriz riesgos de seguridad digital Plantilla-v1-2022 se puede evidenciar para la planificacion y control operacional. En ella se puede visulizar los controles para reducir y mitigar los riegos relaconados con los requisitos de seguridad y privacidad de la
	9	Realizar Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	NO			1	Informe	ANUAL	Este tipo de informacion de ejcución del plan de tratamiento puede ser evidenciada en la sección de seguimiento al plan de tratamiento de la matriz de riegos digitales , que se encuentra cargada en el aplicativo isolución.
	10	Hacer documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	NO			1	Documento	ANUAL	Se encuentran registrados los indicadores de gestión del proceso de Gestión de Innovación Digital, donde se incluyen seguridad y privacidad de la información. Pero no se encuentra un documento descriptivo.
	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	Se encuentra el documento cargado como registro en el aplicativo isolución con el nombre de "Plan general de transicion para adopcion IPV6-UCEVA-2021"
Evaluación	12	Construcción del Plan de revisión y seguimiento, a la implementación del MSPI	NO			1	Plan	ANUAL	Se cuenta con un cronograma de implementación , en el cual se puede evidenciar la meta, entregable, la fechas y el porcentaje de ejecución
	13	Construcción del Plan de Ejecución de Auditorias	NO			1	Plan	ANUAL	Existe el procedimiento de auditoría al sistema integrado **GMC-GSSI-D005**
Mejora	14	Construcción del Plan de mejora continua	NO			1	Plan	ANUAL	Existe el procedimiento de acción preventiva y oportunidad de mejora **GMC-GSSI-D002**

8 SEGUIMIENTO

Para efectos de seguimiento al presente Plan de Seguridad y Privacidad de la Información 2023, 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 2 Matriz de Seguimiento y Articulación con Plan de Acción Institucional 2023

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**	**Periodo de Ejecución**	**Observaciones**
Planeación	**1**	Actualizar la Matriz con la identificación, valoración y clasificación de activos de información.	NO			1	Matriz	Tercer Trimestre	
	2	Actulizar Documento con la caracterización de activos de información, que contengan datos personales	NO			1	Matriz	Tercer Trimestre	
	3	Actualizar el Inventario de activos de IPv6	SI	INVERSIÓN	Innovación TIC para el fortalecimiento Insttitucional de la Unidad central del valle del cauca durante la vigencia 2023	1	Documento	Cuarto Trimestre	
	4	Realizar la Integración del MSPI, con el sistema de gestión documental de la entidad.	SI	INVERSIÓN	Innovación TIC para el fortalecimiento Insttitucional de la Unidad central del valle del cauca durante la vigencia 2023	1	Proceso de integración	Cuarto Trimestre	
	5	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.	NO			2	Matriz	Cuarto Trimestre	
Implementación	**6**	Realizar Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	NO			1	matriz	Cuarto Trimestre	
Evaluación	**7**	Construcción del Plan de Ejecución de Auditorias	NO			1	plan	Cuarto Trimestre	
Mejora	**8**	Construcción del Plan de mejora continua	NO			1	plan	Cuarto Trimestre	