Institución de Educación Superior
UCEVA
Unidad Central del Valle del Cauca

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2023

Historial de Revisiones

Fecha	Versión	Descripción	Autor
03/07/2019	1.0	Creación del documento	Maritza Beltrán García
12/03/2020	1.1	Actualización	Juan Carlos Tascón Restrepo
14/01/2021	1.2	Actualización	Juan Carlos Tascón Restrepo
19/11/2021	1.3	Actualización	Juan Carlos Tascón Restrepo
2/12/2022	1.4	Actualización	Paola Andrea Palacios Mosquera

CONTENIDO

ILUSTRACIONES

TABLAS

INTRODUCCIÓN

La gestión del riesgo de la seguridad de la información tiene como estándar internacional la norma ISO 27005:2018, en la cual se pueden encontrar las pautas y procedimientos para el tratamiento del riesgo. (ISO, 2018).

La Gestión de riesgos es fundamental para la toma de decisiones en el marco de Seguridad dentro del Modelo de Seguridad y Privacidad de la información. Como otro punto, la metodología en que se soporta esta guía es la "Guía de Riesgos" del DAFP, tratando que exista una integración con demás modelos de Gestión a lo trabajado dentro de la institución, aprovechando el trabajo realizado en la identificación de Riesgos para ser integrados con los Riesgos de Seguridad de acuerdo al "Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018"(MINTIC, 2018).

Al alinear los Objetivos estratégicos de la Institución, con la realización del Modelo de Seguridad y Privacidad de la información, se alcanza una integración con lo estipulado en la de la guía de Riesgos del DAFP, igualmente con lo determinado en otros modelos de Gestión como es el caso de MIPG.

Es significativo destacar que para la evaluación de riesgos en seguridad de la información un producto importante es la clasificación de activos de información, debido a que es fundamental ejecutar la gestión de riesgos a los activos de información hallados con clasificación ALTA y MEDIA considerando los criterios de clasificación y aplicando el "Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018"; como se muestra en la siguiente Tabla.

Tabla 1. Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: Guía Gestión de Riesgos MINTIC (articles-5482_G7_Gestion_Riesgos, 2016)

Tabla 2. Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Guía Gestión de Riesgos MINTIC (articles-5482_G7_Gestion_Riesgos, 2016)

No tener implementada la gestión de la seguridad de la información en la Unidad Central del Valle del Cauca, UCEVA, se expone a la perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información Institucional.

Este documento contiene las fases para la implementación del Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para el año 2022 - 2023, alineado con la política de Gobierno Digital

del estado colombiano; busca mitigar las posibles afectaciones a los activos de información institucional, basándose en la metodología de riesgos ver 5, planteada por DAFP (2020).

1. MARCO NORMATIVO

En este literal, se referencia el marco normativo actual que tiene relación con la gestión de TI en el estado.

Tabla 3. Relación de Normatividad Gestión TI

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".

Marco Normativo	Descripción
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 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

Marco Normativo	Descripción
	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".
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

Marco Normativo	Descripción
	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".
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

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Proporcionar las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza y reducir la vulnerabilidad del sistema o el posible impacto en la institución.

3.2. OBJETIVOS ESPECÍFICOS

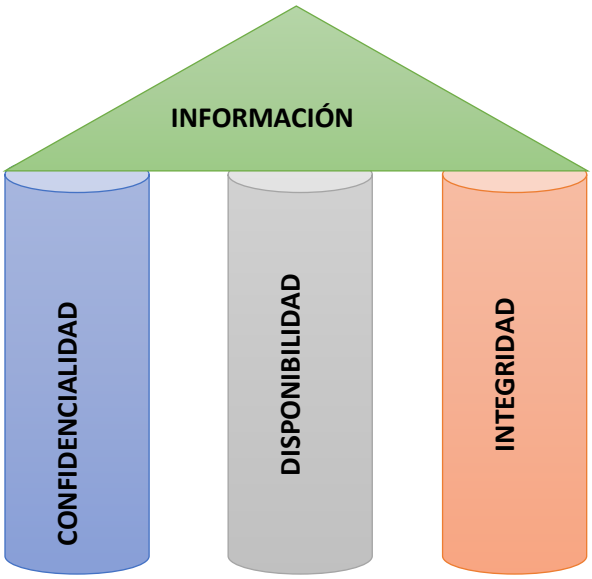
- Precisar la metodología, etapas y acciones para la implementación del plan.
- Identificar los riesgos existentes en la institución y sus posibles causas.
- Valorar los riesgos identificados en la institución.
- Instaurar controles y políticas que generen la confidencialidad integridad y disponibilidad de los activos información.

4. MARCO TEORICO

4.1. SEGURIDAD INFORMÁTICA

La seguridad de la información es la agrupación de acciones preventivas y reactivas que se realizan a la altura tanto de la Institución como en los sistemas tecnológicos, con el propósito de asegurar la información tratando de conservar inalterables los pilares de confidencialidad, disponibilidad e integridad.

lustración 1. Pilares de la información



Fuente: Elaboración propia con base en PTRSPI-UCEVA (2020).

4.2. NORMA ISO 27001

Es una norma internacional que refiere cómo tratar la Seguridad de la Información de una empresa a mediante la aplicación de una metodología.

4.3. NORMA ISO 27005

Es un estándar internacional que se dedica a la gestión de riesgos de seguridad de la información y se compone de 18 secciones. Esta norma es un apoyo para la ISO 27001.

Las secciones contenidas en la norma ISO 27005(2018) son:

1) Prefacio;2) Introducción; 3) Referencias normativas; 4) Términos y definiciones; 5) Sección estructura; 6) Sección fondo; 7) Descripción general del proceso de ISRM; 8) Establecimiento de contexto. 9) Evaluación de riesgos de seguridad de la información. 10) Tratamiento de riesgos de seguridad de la información. 11) Seguridad de la información aceptación del riesgo; 12) Seguridad de la información comunicación de riesgo. 13)Seguridad de la información monitoreo y revisión de riesgos; 14) Anexo A: Definición del alcance del proceso. 15)Anexo B: Valoración de activos y evaluación de impacto. 16) Anexo C: ejemplos de amenazas típicas. 17) Anexo D: Vulnerabilidades y métodos de evaluación de vulnerabilidad. 18)Sección Anexo E: enfoques ISRA. ISO 27005(2018).

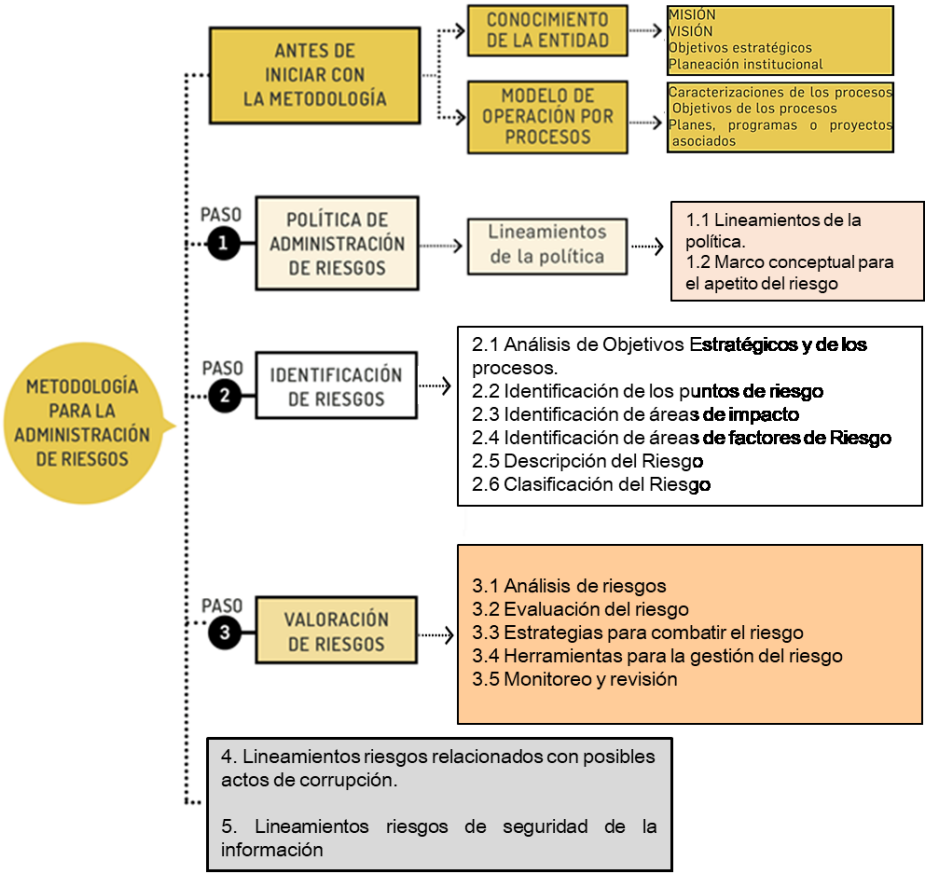
4.4. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Selección de las mejores prácticas, para surtir requisitos para el ciclo de vida PHVA de la gestión del riesgo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital.

4.5. GUÍA DE GESTIÓN DE RIESGOS – MINTIC

Con esta guía alinean los objetivos estratégicos de la Entidad, a la ejecución del MSPI con lo cual se alcanzará una integración con lo estipulado en la metodología de Riesgos del DAFP y el “Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018”, así como lo determinado en otros modelos de Gestión como es el caso de MIPG.

lustración 2. Proceso para la administración del riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI. MINTIC (articles-5482_G7_Gestion_Riesgos, 2016).

Tabla 4. Etapas de la Gestión del Riesgo a lo Largo del MSPI

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

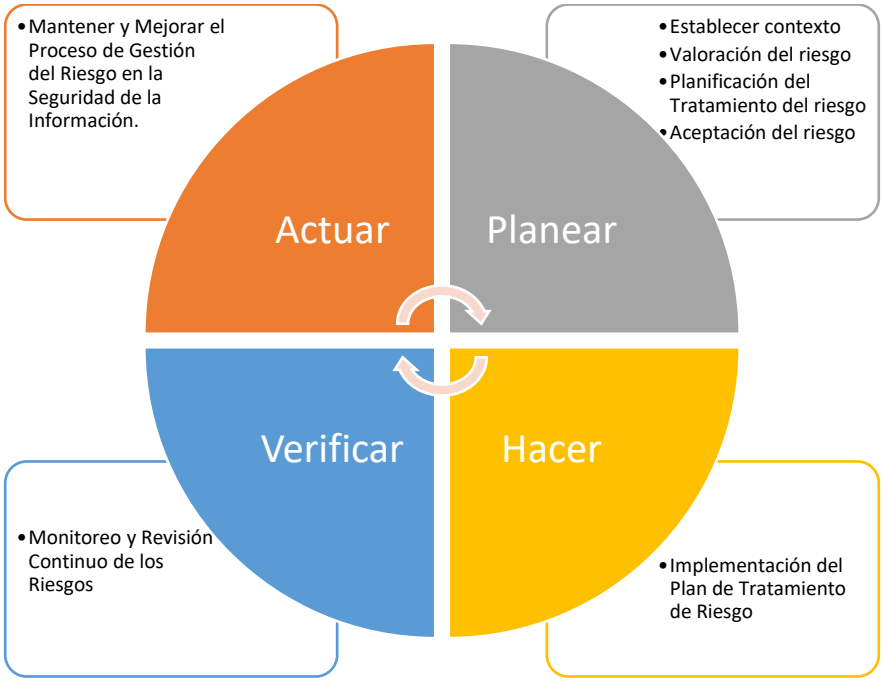
Fuente: Guía Gestión de Riesgos MINTIC - 2016

4.6. CICLO PHVA (PLANEAR, HACER, VERIFICAR, ACTUAR)

Es una herramienta de gestión presentada en los años 50 por el estadístico estadounidense Edward Deming. Aunque podría pensarse, por su antigüedad, que ha perdido vigencia ocurre todo lo contrario, se encuentra plenamente vigente, y es así como ha sido adoptado por varias normas de la familia ISO porque ha demostrado eficacia en las organizaciones para el mantenimiento de sus procesos de forma continua, progresiva y en constante mejora. (PTRSPI, 2020).

El ciclo PHVA logra enmarcar la gestión del riesgo dentro de la seguridad de la información, que se establece en el Modelo de Seguridad y Privacidad de la Información – MSPI, así:

lustración 3. MSPI alineado con el Ciclo PHVA



Fuente: Elaboración propia (PTRSPI, 2020)

5. FASES DE IMPLEMENTACIÓN

La alta dirección tiene que asumir la responsabilidad de facilitar el cumplimiento de los objetivos en lo referente a la gestión del riesgo de seguridad y privacidad de la información, por medio de la instauración de políticas, roles y responsabilidades, y la asignación de recursos que se necesiten para que el proceso se ejecute de una manera efectiva en la institución.

5.1. PLANEAR

Contiene los Pasos 1, 2 y 3 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5, emitida por la Función Pública.

Paso 1: política de administración de riesgos.
Paso 2: identificación del riesgo.
Paso 3: valoración del riesgo.

5.2. HACER

En esta fase se implementan los planes de tratamiento de riesgos definidos.
La Línea Estratégica tiene que proveer los recursos que se necesiten para dar comienzo al tratamiento de los riesgos.
El encargado de la seguridad digital tendrá que supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes realicen las actividades planteadas.

5.3. VERIFICAR

Se debe ejecutar el Monitoreo y revisión por medio de las tres líneas de defensa estipuladas en MIPG en la Dimensión 7 Control Interno, de los planes de tratamiento para determinar su efectividad.

Las líneas de defensas son:

- **Línea Estratégica**

Corresponde al Comité de Auditoría de las Empresas Industriales y Comerciales del Estado y/o a los comités institucionales de coordinación de control interno establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo. (Guía para la administración del riesgo – DAFP, 2020)

- **Primera Línea Estratégica**

Corresponde a los jefes de área y/o grupo (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades. (Guía para la administración del riesgo – DAFP, 2020)

- **Segunda Línea Estratégica**

Corresponde al área encargada de la gestión del riesgo (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación. (Guía para la administración del riesgo – DAFP, 2020)

- **Tercera Línea Estratégica**

Les corresponde a las unidades de control interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo. (Guía para la administración del riesgo – DAFP, 2020)

5.4. ACTUAR

Con el Mejoramiento continuo de la gestión del riesgo de seguridad digital, se garantiza la gestión de riesgos de seguridad digital, por consiguiente, se establecerá que cuando existan hallazgos, falencias o incidentes de seguridad digital se debe mitigar el impacto de su existencia y tomar acciones para controlarlos y prevenirlos. Igualmente, igualmente debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse. (PTRSPI,2020).

6. EJECUCION DEL CRONOGRAMA 2022

6.1. DEFINICIÓN DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGO.

La alta dirección en la Resolución Rectoral 1457 de 2019, estableció la política de administración del riesgo.

6.2. DEFINICIÓN DEL CONTEXTO INTERNO, EXTERNO Y DE LOS PROCESOS DE LA ENTIDAD PÚBLICA.

La oficina de informática y telemática, en la matriz DOFA definió el contexto del área. Fuente Herramienta para la construcción del Plan Estratégico de Tecnologías de la Información - PETI.

6.3. IDENTIFICACIÓN DE ACTIVOS.

Es responsabilidad de todas las áreas realizar la identificación, clasificación y gestión de los activos de información**,** referenciándolos en el formato denominado ***Inventario de Activos de Información*** **GDI-GSIN-F-037**. La oficina de informática y telemática realizó el proceso con los activos de información de hardware, software e información.

En el año 2022 se creó grupo de trabajo integrado por la oficina de control interno disciplinario, Oficina de planeación, Gestión documental e Informática y telemática, para la capacitación y el acompañamiento del diligenciamiento del formato inventario de activos de información y se estableció un cronograma por dependencias para su actualización con su criticidad y realizar el tratamiento de los riesgos; los archivos se organizaron de acuerdo a las tablas de retención documental y se dio cumplimiento al cronograma estipulado. Es de aclarar que solo fueron enviados 20 archivos por las dependencias.

6.4. IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DE LOS RIEGOS DE ACTIVOS.

La oficina de informática y telemática, ejecutó el proceso de actualización, análisis y valoración de los riesgos de los activos de información del año 2022, y se realizó el seguimiento a los 8 planes de mejoramiento establecidos en la matriz de riesgos.

Tabla 5 Matriz de Seguimiento y Articulación con Plan de Acción Institucional 2022

Caracterización					*Medición*				*Seguimiento*	
No.	**Actividad a realizar**	**¿Requiere presupuesto?**	**Si requiere presupuesto, especifique de qué tipo (Funcionamiento / Proyecto de**	**Si seleccionó de inversión ¿A que proyecto de inversión**	**Meta**	**Indicadores**	**Temporalidad de medición**	**Observaciones**	**Cumplimiento Meta**	**Observaciones**
1	Realizar la Identificación y actualización de activos de información	NO			1	Documentos de identificación y actualización	ANUAL		1	La identificación se encuentra a través del registro de información de la vigencia 2022 . En la url https://www.uceva.edu.co/transparencia/instrumentos-gestion-informacioninstrumentos-gestion-informac-publicar se encuentran los activos de informacion desde el año 2020 hasta el año 2022 de la oficina de informática
2	Identificación de riesgos	NO			1	Matriz de Identificación de ries	ANUAL		1	Se encuentra publicada en ISOLUCION como registro con el nombre "Matriz riesgos de seguridad digital Plantilla-v1-2022"
3	Efectuar la valoración de riesgos.	NO			1	Matriz de Valoración de riesgo	ANUAL		1	Se encuentra publicada en ISOLUCION como registro "Matriz riesgos de seguridad digital Plantilla-v1-2022"
4	Hacer la implementación plan de tratamiento de riesgos	NO			8	Planes de mejoramiento	ANUAL		8	Se realiaron 8 planes de mejoramiento y su seguimiento se encuentra evidenciado en la matriz de riesgos digitales que esta cargada en el aplicativo isolucion como un registro "Matriz riesgos de seguridad digital Plantilla-v1-2022"
5	Ejecutar Monitoreo y Revisión	NO			4	Seguimientos a los riesgos	ANUAL		1	Se realiza un seguimiento anual y esta evidenciado en la matriz de riesgos digitales que esta cargada en el aplicativo isolucion como un registro "Matriz riesgos de seguridad digital Plantilla-v1-2022"
6	Comunicación y Consulta	NO			1	Evidencia en Isolución	ANUAL		1	Se puede evidenciar en el aplicativo Isolución en el listado maestro de registros con el archivo "Evidencia de Cominicación y consulta Riesgos Digitales" y la "Matriz riesgos de seguridad digital Plantilla-v1-2022"

7. CRONOGRAMA

El siguiente cronograma se estableció para el año 2023.

Tabla 6. Cronograma 2023

Actividad	Responsable	Ene -Mar 2023	Abr -Jun 2023	Jul -Sept 2023	Oct -Dic 2023
Identificación y actualización de activos de información	Jefe de Oficina de Informática y Telemática				
Actualización de matriz de riesgos.	Jefe de Oficina de Informática y Telemática				
identificación, Valoración y plan tratamiento de riesgos.	Jefe de Oficina de Informática y Telemática				
implementación plan de tratamiento de riesgos	Jefe de Oficina de Informática y Telemática				
Monitoreo y Revisión	Jefe de Oficina de Informática y Telemática				
Comunicación y Consulta	Jefe de Oficina de Informática y Telemática				

8. SEGUIMIENTO

Para efectos de seguimiento al presente Plan de Tratamiento de Riesgos 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 7 Matriz de Seguimiento y Articulación con Plan de Acción Institucional 2023

Caracterización					*Medición*			
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**
1	Identificación y actualización de activos de información	NO			1	Matriz de identificación y actualización de activos	Segundo Trimestre	
2	Actualización de matriz de riesgos.	NO			1	Matriz de riesgos	Primer Trimestre	
3	identificación , Valoración y plan de tratamiento de riesgos.	NO				Si se identifica un nuevo riesgo	Cuarto Trimestre	
4	implementación plan de tratamiento de riesgos	NO			1	Matriz de riesgos	Cuarto Trimestre	
5	Monitoreo y Revisión	NO			1	Seguimientos a los riesgos	Cuarto Trimestre	
6	Comunicación y Consulta	NO			1	Evidencia en Isolución	Cuarto Trimestre	