Institución de Educación Superior
UCEVA
Unidad Central del Valle del Cauca

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

2022

OFICINA DE INFORMÁTICA Y TELEMÁTICA

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

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. (MINTIC, 2016).

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 modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas”; 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 2021 - 2022, 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 1OBJETIVOS

1.1 OBJETIVO GENERAL

Reducir los riesgos de seguridad y privacidad de la información en los procesos institucionales.

1.2 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.

2 2MARCO 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

Normativa	Descripción
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 594 de 2000	“Por medio de la cual se dicta la Ley General de Archivos 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”.
Ley 734 de 2002	“Por la cual se expide el código disciplinario único”.
Ley 962 de 2005	“Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o presten servicios públicos”.
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 1474 de 2011	“Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. En su artículo 74 impone a las Entidades públicas la obligación de publicar en su respectiva página web, el Plan de Acción para el año siguiente, en el marco de las políticas establecidas para fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”.

Normativa	Descripción
Ley 019 de 2012	"Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, hace referencia al uso de medios electrónicos como elemento necesario en la optimización de los trámites ante la Administración Pública y establece en el artículo 4° que las autoridades deben incentivar el uso de las tecnologías de la información y las comunicaciones a efectos de que los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas".
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".
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 2573 de 2004	"Adopción de la norma técnica de calidad de la gestión pública".
Decreto 4485 de 2009	"Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública. Se adopta la Norma Técnica de Calidad en la Gestión Pública NTCGP 1000:2009, la cual determina las generalidades y los requisitos mínimos para establecer, documentar, implementar y mantener un Sistema de Gestión de la Calidad en los organismos, entidades y agentes obligados".
Decreto 235 de 2010	"Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas (Ley 2550 de 1995)".
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 2578 de 2012	"Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los Archivos del Estado".
Decreto 2609 de 2012	"Por la cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 2618 de 2012	"Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones 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 0032 de 2013	"Por la cual se crea la Comisión Nacional Digital y de Información Estatal".

Normativa	Descripción
Decreto 943 de 2014	“Por medio del cual de adopta la actualización del Modelo Estándar de Control Interno para el Estado Colombiano”.
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 1078 de 2015	“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Y especialmente en sus artículos a partir del 2.2.9.1.1.1. titulo 9. Define los lineamientos, instrumentos y plazos de la estrategia de gobierno en línea para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones”.
Decreto 1413 de 2017	“Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales”.
Acuerdo 006 de 2014 del AGN	“Por medio del cual se desarrollan los artículos 46,47 y 48 del Título XI de "Conservación de documentos" de la Ley 594 de 2000". Define el Sistema Integrado de Conservación SIC, componentes, formulación de los planes del SIC, programas de conservación preventiva. Capitulo III: Plan de Preservación digital a largo plazo”.
Acuerdo 003 de 2015 del AGN- Documento electrónico	“Por el cual se establecen los lineamientos generales para las Entidades del Estado en cuanto a la gestión electrónica de documentos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de 594 de 2000 y el capítulo IV del Decreto 2609 de 2012”.
CONPES 3670 de 2010.	“Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones”.
CONPES 3701 de 2011	“Lineamientos de Política para Ciberseguridad y Ciber defensa”.
Decreto 1008 del 14 de junio 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”.

3 MARCO TEORICO

3.1 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).

3.2 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.

3.3 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).

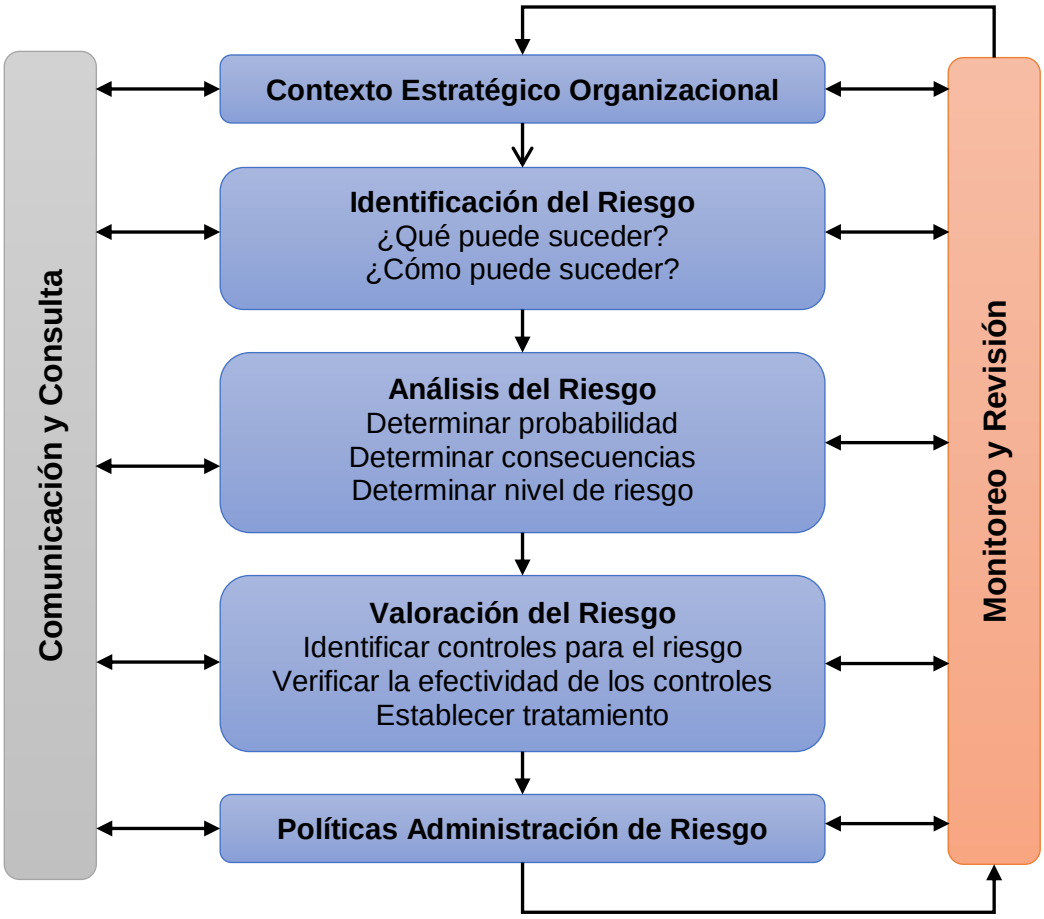
3.4 Modelo de seguridad y privacidad de la información

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.

3.5 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 modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas”, así como lo determinado en otros modelos de Gestión como es el caso de MIPG.

lustración 2 Proceso para la administración del riesgo



Fuente: Guía para la administración del riesgo – DAFP

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.

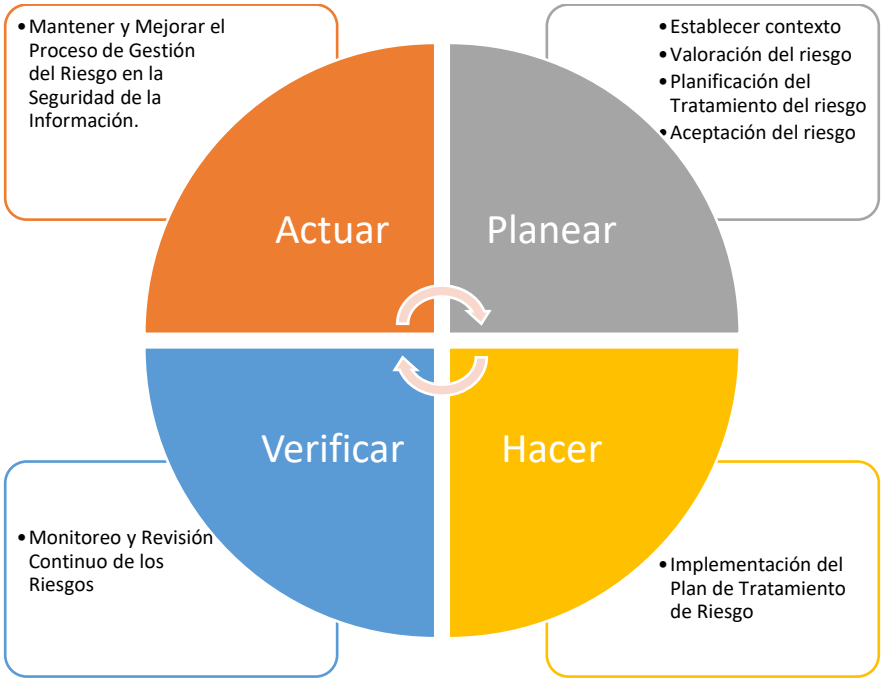
Fuente: Guía Gestión de Riesgos MINTIC - 2016

3.6 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)

4 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.

4.1 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.

4.2 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.

4.3 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)

4.4 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).

5 CRONOGRAMA

El siguiente cronograma se estableció para el año 2022.

Actividad	Responsable	Ene -Mar 2022	Abr -Jun 2022	Jul -Sept 2022	Oct -Dic 2022
Identificación y actualización de activos de información	Jefe de Oficina de Informática y Telemática				
Identificación de riesgos.	Jefe de Oficina de Informática y Telemática				
Valoración 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				

6 EJECUCION DEL CRONOGRAMA

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 archivo denominado ***Inventario de Activos de Información*** **GDI-GIDI-F-002**. La oficina de informática y telemática realizó el proceso con los activos de información de hardware, software e información.

6.4 Identificación, Análisis y Valoración de los Riegos de Activos.

La oficina de informática y telemática, ejecutó el proceso de identificación, análisis y valoración de los riesgos de los activos de información del año 2021, estableciendo los controles y los planes de mejoramiento.

7 7SEGUIMIENTO

Para efectos de seguimiento al presente Plan de Tratamiento de Riesgos 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 5 Matriz de Seguimiento y Articulación con Plan de Acción Institucional 2022

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**	**Temporalidad de medición**	**Observaciones**
1	Realizar la Identificación y actualización de activos de información	NO			1	Documentos de identificación y actualización	ANUAL	
2	Identificación de riesgos	NO			1	Matriz de Identificación de riesgos	ANUAL	
3	Efectuar la valoración de riesgos.	NO			1	Matriz de Valoración de riesgos	ANUAL	
4	Hacer la implementación plan de tratamiento de riesgos	NO				Sólo si aplica	ANUAL	
5	Ejecutar Monitoreo y Revisión	NO			4	Seguimientos a los riesgos	ANUAL	
6	Comunicación y Consulta	NO				Evidencia en Isolución	ANUAL	