UNIDAD CENTRAL DEL VALLE DEL CAUCA

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

Versión 1.1

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

CONTENIDO

ILUSTRACIONES

TABLAS

INTRODUCCIÓN

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

La norma ISO 27005:2011 es un estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información. Contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera. Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo mediante el plan de tratamiento de riesgos.

Dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (en adelante MSPI), un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Por otra parte, Teniendo en cuenta que el contexto organizacional de esta guía y del MSPI en sí, son las entidades del Estado, la metodología en la cual se basa la presente guía es la “Guía de Riesgos” del DAFP1, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión, y de éste modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad.

Es así como alineando los Objetivos estratégicos de la Entidad, al desarrollo del MSPI se logra una integración con lo establecido a través de la guía de Riesgos del DAFP, así como con lo determinado en otros modelos de Gestión por ejemplo MIPG.

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

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

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

El no contar con una buena gestión de la seguridad de la información, para La Unidad Central del Valle del Cauca, UCEVA puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

El presente documento plantea el proceso de implementación del Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para la vigencia 2019 – 2020, alineado con la política de Gobierno Digital del estado Colombiano; busca mitigar las posibles afectaciones a los activos de información institucional, utilizando un enfoque basado en la gestión de riesgos, que permita maximizar la confidencialidad, integridad y disponibilidad de dichos activos.

1 OBJETIVO

Minimizar los riesgos asociados a la seguridad y privacidad de la información en los procesos institucionales.

1.1 OBJETIVOS ESPECÍFICOS

- Definir la metodología, fases y actividades para la implementación del plan.
- Identificar los riesgos actuales y sus posibles causas.
- Establecer controles y políticas de seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.

.

2 MARCO NORMATIVO

El PETI de la Unidad Central del Valle del Cauca se encuentra alineado al marco normativo vigente para el sector educativo, instituciones de educación superior y la función pública del estado colombiano. A continuación, se hace referencia a las principales normas relacionas con la gestión de TI en el estado y del sector educativo, Instituciones de Educación Superior – IES.

Ley 39 de 1981. Sobre microfilmación y certificación de archivos.

Ley 152 de 1994. Por la cual se establece la Ley Orgánica del Plan de Desarrollo. Tiene como propósito establecer los procedimientos y mecanismos para la elaboración, aprobación, ejecución, seguimiento, evaluación y control de los planes de desarrollo, así como la regulación de los demás aspectos contemplados por el artículo 342, y en general por el artículo 2 del Título XII de la constitución Política y demás normas constitucionales que se refieren al plan de desarrollo y la planificación.

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 872 de 2003. "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".

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 1437 de 2011. Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. En su Parte Primera tienen como finalidad

proteger y garantizar los derechos y libertades de las personas, la primacía de los intereses generales, la sujeción de las autoridades a la Constitución y demás preceptos del ordenamiento jurídico, el cumplimiento de los fines estatales, el funcionamiento eficiente y democrático de la administración, y la observancia de los deberes del Estado y de los particulares."

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.

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 1564 de 2012. Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. Tiene por objeto regular la actividad procesal en los asuntos civiles, comerciales, de familia y agrarios. Se aplica, además, a todos los asuntos de cualquier jurisdicción o especialidad y a las actuaciones de particulares y autoridades administrativas, cuando ejerzan funciones jurisdiccionales, en cuanto no estén regulados expresamente en otras leyes.

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 1740 de diciembre 23 de 2014. Por la cual se desarrolla parcialmente el artículo 67 y los numerales 21, 22 y 26 del artículo 189 de la constitución política, se regula la inspección y vigilancia de la educación superior, se modifica parcialmente la ley 30 de 1992 y se dictan otras disposiciones.

Ley 1755 de 2015. “Por medio de la cual se regula el derecho fundamental de petición y se sustituye un título del código de procedimiento administrativo y de lo contencioso administrativo”.

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 19 de 2012 Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Decreto 2482 de 2012. "Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión (Ley 489 de 1998, Ley 552 de 1994)".

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".

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 1075 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector Educación.

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 415 de 2016 Por el cual adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015. estableció los lineamientos

para la implementación de la figura de Director de Tecnologías y Sistemas de Información, quien será pieza clave en la construcción de un Estado más eficiente y transparente gracias a la gestión estratégica de las Tecnologías de la Información y las Comunicaciones (TIC). Y en su Artículo 2.2.35.3. Objetivos del fortalecimiento institucional. Para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere el presente decreto, deberán: Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado.

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.

Decreto 1499 de 2017 por el cual se modifica el Decreto 1083 de 2015- Decreto Único Reglamentario del Sector Función Pública. Se integra el Comité Institucional de Gestión y Desempeño: liderado por el viceministro o subdirector de departamento administrativo, y en el nivel descentralizado por los secretarios generales o administrativos. Estará a cargo de orientar la implementación y evaluación de MIPG en cada entidad u organismos público. La Secretaría Técnica

será ejercida por el jefe de la oficina de planeación de la respectiva entidad o quien haga sus veces. Este Comité sustituye los demás comités que tengan relación con los sistemas que se integran en el Sistema de Gestión y el Modelo y que no sean obligatorios por mandato legal. En el orden territorial el representante legal de cada entidad definirá la conformación del Comité Institucional, el cual será presidido por un servidor del más alto nivel jerárquico, e integrado por servidores públicos del nivel directivo o asesor.

Directiva Presidencial 9 de 2010. Establece la obligación que tienen las Entidades públicas de ajustar anualmente sus planes sectoriales e institucionales.

Acuerdo 11 de 1996. "Por el cual se establecen criterios de conservación y organización de documentos".

Acuerdo 047 de 2000. "Por el cual se desarrolla el artículo 43 del capítulo V "Acceso a los documentos de archivo", del Reglamento general de archivos sobre "Restricciones por razones de conservación".

Acuerdo 50 de 2000. "Por el cual se desarrolla el artículo 64 del título VII "conservación de documento", del Reglamento general de archivos sobre "Prevención de deterioro de los documentos de archivo y situaciones de riesgo".

Acuerdo 037 de 2002. "Por el cual se establecen las especificaciones técnicas y los requisitos para la contratación de los servicios de depósitos, custodia, organización, reprografía y conservación de documentos de archivo en desarrollo de los artículos 13 y 14 y sus Parágrafos 1 y 3 de la Ley General de Archivos 594 de 2000".

Acuerdo 004 de 2013 del AGN. Por el cual se reglamenta parcialmente los Decretos

2578 y 2609 de 2012 y se modifica el procedimiento para la elaboración, presentación, evaluación, aprobación e implementación de la Tablas de Retención Documental y Tablas de Valoración Documental. Art.14. Actualización. Cuando se transformen tipos documentales físicos en electrónicos. Art. 18. Usos de tecnologías de información que permitan la automatización de la elaboración, consulta y actualización de la TRD, de forma que facilite la interoperabilidad con el “Registro Único de Series Documentales” y otros sistemas de información de cada entidad.

Acuerdo 005 de 2013 del AGN. Por el cual se establecen los criterios básicos para la clasificación, ordenación y descripción de los archivos en las entidades públicas y privadas que cumplen funciones públicas y se dictan otras disposiciones. Art. 20. Utilización de medios.

Acuerdo 002 de 2014 del AGN - "Por medio del cual se establecen los criterios básicos para creación, conformación, organización, control y consulta de los expedientes de archivo y se dictan otras disposiciones”.

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".

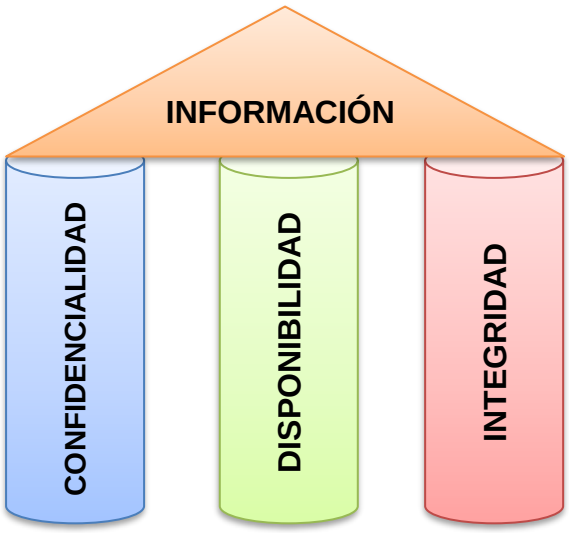
Decreto 1008 del 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

3 MARCO TEORICO

3.1 SEGURIDAD INFORMÁTICA

La seguridad de la información es el conjunto de medidas preventivas y reactivas que se implementan a nivel tanto de la Institución como los sistemas tecnológicos, con el objetivo de resguardar y proteger la información buscando mantener inquebrantables los pilares de confidencialidad, disponibilidad e integridad.

lustración 1 Pilares de la información



Fuente: Elaboración propia

3.2 NORMA ISO 27001

Es un estándar internacional que describe cómo implementar el Sistema de Gestión de Seguridad de la Información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

3.3 NORMA ISO 27005

Es un soporte a la norma ISO 27001, la cual proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica.

Las secciones contenidas en la norma ISO 27005 son:

- Prefacio
- Introducción
- Referencias normativas
- Términos y definiciones
- Estructura

- Fondo
- Descripción general del proceso de ISRM
- Establecimiento de contexto
- Evaluación de riesgos de seguridad de la información (ISRA)
- Tratamiento de riesgos de seguridad de la información
- Seguridad de la información Aceptación del riesgo
- Seguridad de la información Comunicación de riesgos
- Seguridad de la información Monitoreo y revisión de riesgos
- Anexo A: Definición del alcance del proceso
- Anexo B: Valoración de activos y evaluación de impacto
- Anexo C: ejemplos de amenazas típicas
- Anexo D: Vulnerabilidades y métodos de evaluación de vulnerabilidad
- Anexo E: enfoques ISRA"

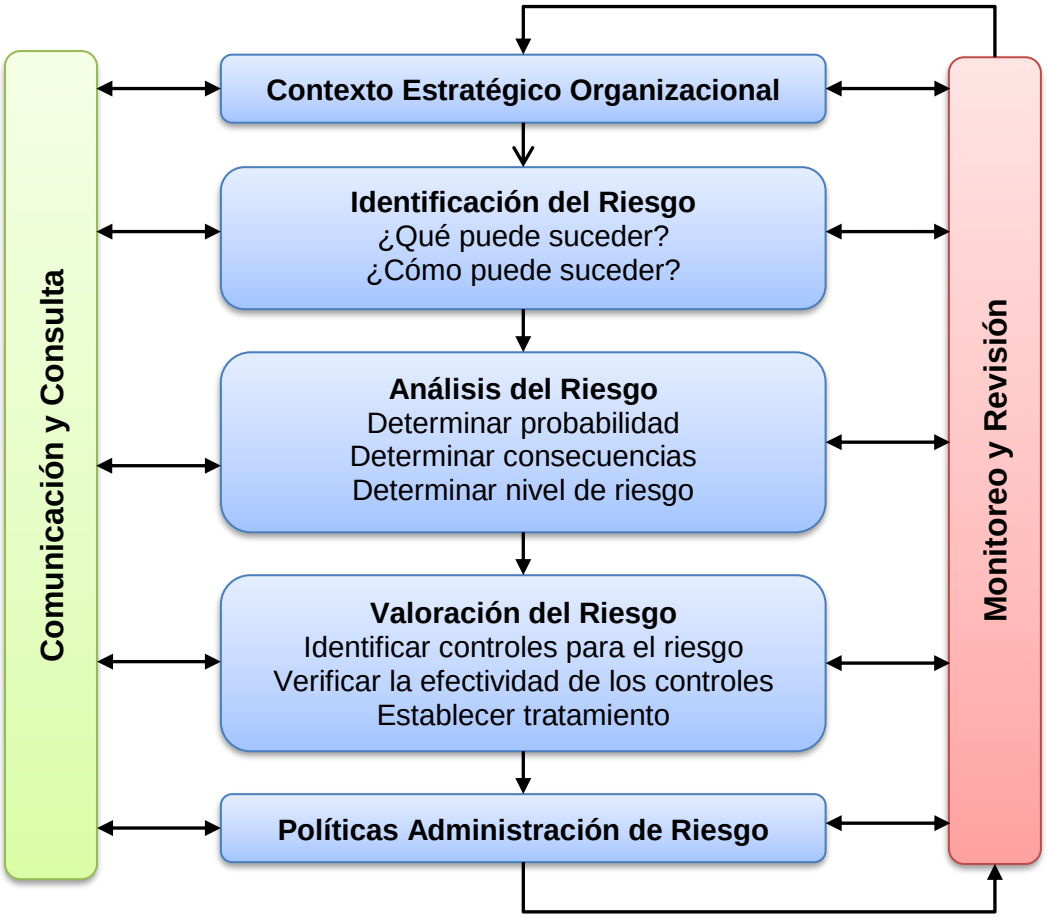
3.4 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL.

3.5 GUÍA DE GESTIÓN DE RIESGOS – MINTIC

Permite la alineación de los objetivos estratégicos de la Entidad, al desarrollo del MSPI para lograr una integración con lo establecido a través de la guía de Riesgos del DAFP, así como con lo determinado en otros modelos de Gestión por ejemplo el 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.

Tabla 3. 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.

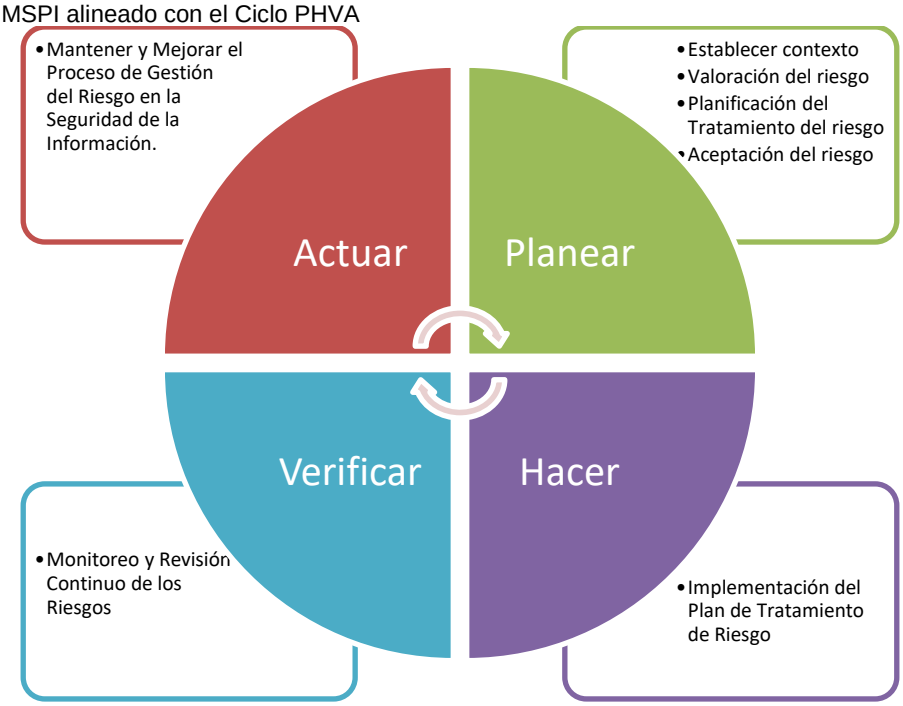
Fuente: Guía Gestión de Riesgos MINTIC

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.

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

4 FASES DE IMPLEMENTACIÓN

La alta dirección debe adquirir el compromiso de facilitar el cumplimiento de los objetivos sobre la gestión del riesgo de seguridad y privacidad de la información, a través del establecimiento de políticas, roles y responsabilidades, y la designación de recursos necesarios para que el proceso se desarrolle en la institución de forma efectiva.

4.1 PLANEAR

Abarca los Pasos 1, 2 y 3 de la Guía para la Administración de los Riesgo de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida por la Función Pública.

4.2 HACER

Con los insumos de la ejecución de la fase anterior, se ejecuta la ruta crítica definida, es decir, se implementan los planes de tratamiento de riesgos definidos.

Aquí la Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes.

4.3 VERIFICAR

Monitoreo y revisión a través de las tres líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, de los planes de tratamiento para determinar su efectividad.

4.4 ACTUAR

Mejoramiento continuo de la gestión del riesgo de seguridad digital, se debe garantizar la mejora continua de la gestión de riesgos de seguridad digital, por lo tanto, debe establecer 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. Adicionalmente, se debe establecer y hacer frente a las consecuencias propias de la no conformidad que llegó a materializarse.

5 CRONOGRAMA

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8
Definición del contexto interno, externo y de los procesos de la entidad pública.								
Definición de la política de administración de riesgo.								
Designación de roles y responsabilidades.								
Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.								
Identificación de activos.								
Identificación de riesgos.								
Valoración de riesgos.								
Definición del tratamiento de los riesgos.								
Monitoreo y Revisión								
Comunicación y Consulta								