UNIVERSIDAD DEL QUINDÍO
Res.MEN 014915 - 02 AGO 2022
RENOVACIÓN ACREDITACIÓN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oficial de Seguridad y Privacidad de la Información

UNIQUINDÍO
en conexión territorial
www.uniquindio.edu.co

INTRODUCCIÓN

La Universidad del Quindío en cumplimiento de las directrices emitidas por el Gobierno Nacional, en lo que respecta a sus políticas de Gobierno Digital y Seguridad Digital; así como, siendo consciente de los riesgos que se generan con el uso de las tecnologías de la información, inició el proceso de adopción del Modelo de Seguridad de la Información - MSPI en la vigencia 2021, adoptando e implementando algunos de los controles técnicos de seguridad de la información para el proceso de Gestión TIC.

En el año 2022, realiza el diagnóstico para verificar el porcentaje de cumplimiento del MSPI donde se evidencia que la entidad alcanza un 39% de acuerdo a la escala de calificación definida por MinTIC; lo que conllevó a conformar un equipo para iniciar con el proceso de planificación y diseño de los controles, políticas y lineamientos que permitieran avanzar en la adopción del MSPI, mediante la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.

Para la vigencia 2023 se inicia con la implementación de los controles, procedimientos y políticas de seguridad de la información, de manera gradual por fases; donde se establece el cronograma de implementación y seguimiento del SGSPI.

Teniendo en cuenta lo anterior, se diseña el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, definiendo el Plan de Seguridad y Privacidad de la Información de la Universidad del Quindío. dicho plan, pretende facilitar la comprensión del proceso de adopción de la seguridad y privacidad de la información en la entidad, de tal forma que permita lograr el mejoramiento continuo del sistema de gestión y una adecuada gestión de los riesgos de seguridad digital y la protección de la privacidad de la información y los datos, de los procesos y demás partes interesadas.

1. OBJETIVOS

General

Definir las actividades de adopción y mantenimiento de la seguridad y privacidad de la información en la Universidad del Quindío a través del ciclo PHVA, de tal forma que permita garantizar el mejoramiento continuo del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI en la entidad.

Específicos

- Dar cumplimiento a los lineamientos del Gobierno Nacional y a lo expedido por el Ministerio de Tecnologías de la información y las Comunicaciones (MinTIC) así como el cumplimiento de los requisitos legales y regulatorios pertinentes, relacionados con la seguridad de la información y la privacidad y protección de datos personales.
- Generar la Cultura de Seguridad de la información, requerida para la operación, puesta en marcha y mantenimiento del SGSPI de la universidad.
- Proteger la información que genera, procesa, transmite, gestiona y almacena la universidad; así como garantizar la disponibilidad de los procesos y sus servicios.
- Evaluar las amenazas actuales y futuras de la información, mediante la gestión de riesgos de seguridad de la información.
- Promover la mejora continua, involucrando a todas las partes interesadas en los procesos de implementación del SGSPI.
- Ofrecer mayor calidad y valor a las partes interesadas, al implementar la seguridad de la información y la privacidad y protección de los datos, en los procesos de la entidad.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad, mediante el diseño de instrumentos que permitan controlar, verificar y hacer seguimiento a todas las fases del ciclo PHVA en la adopción del MSPI en la universidad.
- Establecer la línea base para que la Universidad pueda adoptar de manera gradual el MSPI en todos sus procesos y certificar a largo plazo un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) basado en la Norma ISO/IEC 27001 y los lineamientos definidos por MinTIC.

2. ALCANCE

Este documento aplica a todo el proceso de implementación, operación, mantenimiento y mejora continua del SGSPI en el marco de la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI y en concordancia a lo establecido en el Decreto 612 de 2018, la Política de Gobierno Digital y Seguridad Digital, la Norma ISO/IEC 27001 y demás lineamientos gubernamentales relacionados con este tema: para las vigencias de 2023, 2024 y 2025.

3. MARCO NORMATIVO

A continuación, se listan algunas de las normas más relevantes, que dan soporte a la operación del SGSPI. La totalidad de las normas o los soportes legales y reglamentarios están descritos en el normograma del sistema de gestión:

- **La 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 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 usen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- **Ley 1581 de 2012**: “Por la cual se dictan disposiciones generales para la protección de datos personales”. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

- **Norma ISO/IEC 27001:2013**: Sistemas de Gestión de Seguridad de la Información.

- **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”. Reglamentada parcialmente por el Decreto Nacional 103 de 2015.

- **Decreto Nacional 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 del 26 de 2015:** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- **Documento CONPES 3995 de 2020:** "Política Nacional de confianza y Seguridad Digital".

- **Directiva Presidencial 03 de marzo de 2021:** Por medio de la cual se establecen los "Lineamientos para el uso de servicios en la nube, Inteligencia Artificial, Seguridad Digital y Gestión de datos."

- **Resolución 500 de 2021:** "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

- **Resolución 1519 de 2022 (MinTIC):** "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"

4. DEFINICIONES[1]

A continuación, se listan los términos que podrían usarse dentro del documento con su respectiva definición.

- **Activo de información:** Todo aquello que tiene valor para la entidad, por lo tanto, debe protegerse. De acuerdo con la norma ISO/IEC 27001, los activos de información se clasifican en: información, software, activos físicos, personas, servicios e intangibles como reputación, imagen de la entidad, etc.

- **Confidencialidad**: Que la información solo sea accedida por las personas autorizadas para ello.

[1] Definiciones contenidas en la ISO 27000. Extraídas del sitio web: https://www.iso27000.es/glosario.html

- **Amenaza:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Seguridad informática:** Rama de la seguridad de la información que se enfoca en la protección de la plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan en dicha plataforma.

5. ACTIVIDADES PARA LA ADOPCIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El propósito del Modelo de Seguridad y Privacidad de la Información - MSPI, debe ser adoptado en todos los procesos, servicios y activos de información de la universidad; sin embargo, debido al tamaño de la misma, los recursos que se requieren para dicho proceso y el contexto de la entidad, se implantará a través del proceso de mejora continua y de manera gradual. Por lo tanto el presente documento las diferentes actividades que se surtirán a corto, mediano y largo plazo.

Para llevar a cabo lo anterior, la Universidad del Quindío toma como referencia los lineamientos dados por MinTIC en el Documento Maestro del Modelo de Seguridad y Privacidad de la Información (en adelante MSPI), el cual brinda las directrices para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

De acuerdo con lo anterior, el Plan de Seguridad y Privacidad de la Información contempla el desarrollo de las fases que se presentan a continuación:

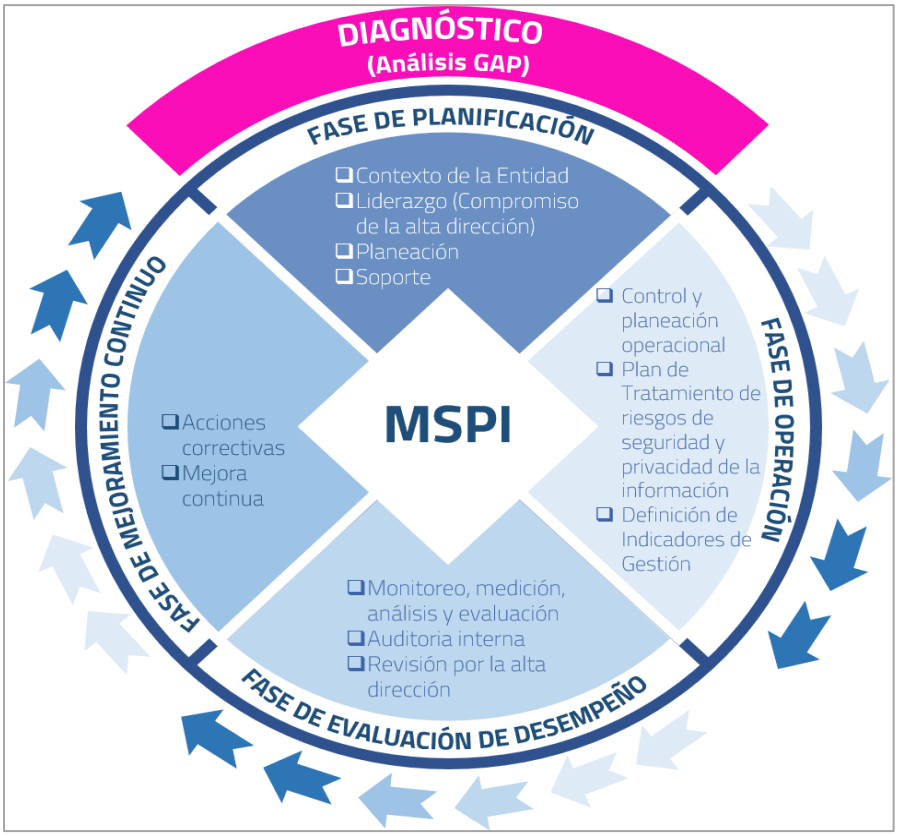


Ilustración 1. Fases de la implementación del MSPI
Fuente: Tomado del Documento Maestro del MSPI[2]

5.1. FASE 1. DIAGNÓSTICO (EN EL CICLO PHVA: PLANEAR)

Como actividad fundamental, para iniciar con el proceso de implementación del MSPI con el esquema del modelo de operación PHVA, se debe desarrollar el diagnóstico para medir el nivel de implementación del modelo en las entidades públicas; dicha herramienta es puesta a disposición por MinTIC en el micrositio de seguridad TI / Modelo de seguridad. La Universidad del Quindío aplicó dicho diagnóstico en la vigencia 2022, encontrando una brecha significativa, lo que obligó al diseño de estrategias para adoptar medidas que permitan incrementar los niveles de implementación del MSPI en la entidad.

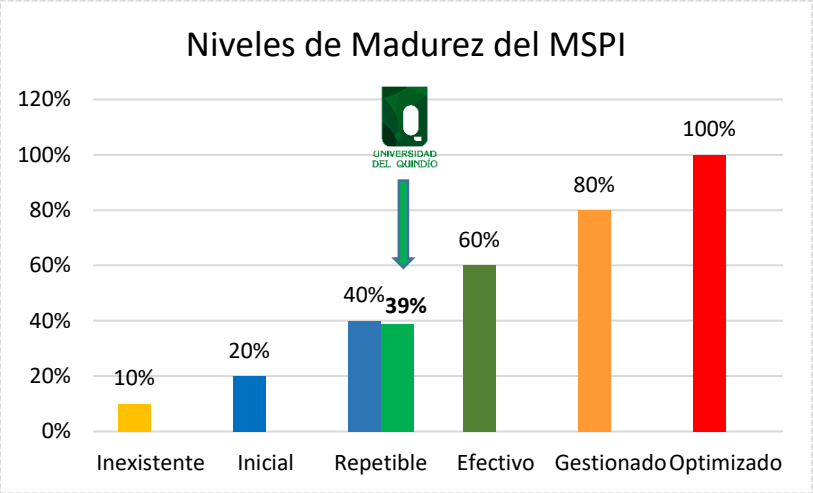
Dichos resultados permitieron a la universidad identificar la línea base y determinar los aspectos con mayor debilidad, para la planeación de las actividades a desarrollar a fin de disminuir la brecha de seguridad; además permite identificar

[2] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf.

específicamente los recursos requeridos en cada fase, los costos, tiempos de implementación, entregables y los hitos que implica y demanda el establecimiento, la operación y la mejora continua del MSPI.

A continuación se detalla el estado en que se encontraba la universidad cuando se aplicó el instrumento de diagnóstico:

Nivel de Madurez de la Universidad del Quindío: Para el análisis y evaluación del cumplimiento de los controles definidos en el anexo A de la norma NTC-ISO/IEC 27001:2013, se realiza la evaluación teniendo en cuenta que no se tiene ninguna exclusión de la totalidad de objetivos de controles y dominios.



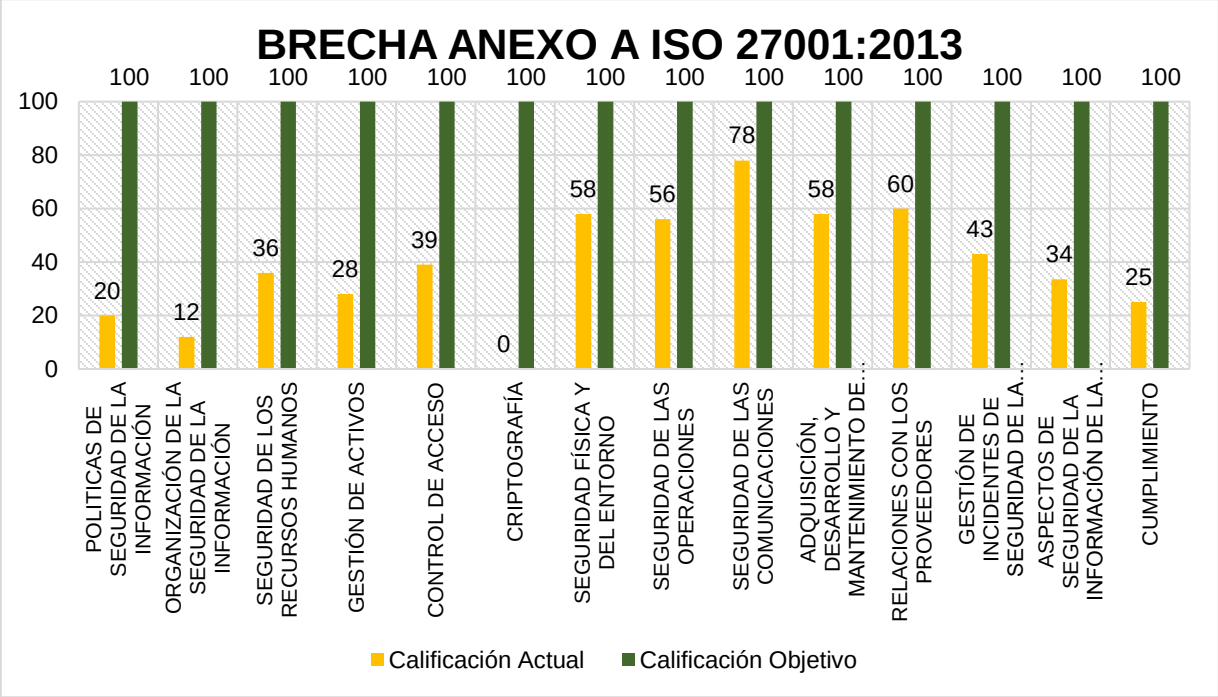
Gráfica 1. Niveles de madurez frente a la implementación del MSPI
Fuente: Propia - Universidad del Quindío

Se identifica un cumplimiento general del MSPI del **39%,** encontrándose en un nivel de madurez **"REPETIBLE"** de acuerdo a la escala de valoración dada por MinTIC, frente a los dominios y controles evaluados. Lo que indica que se evidencian procesos básicos de gestión de seguridad y privacidad, de igual forma existen controles que permiten detectar posibles incidentes de seguridad de la información, pero aún no se encuentran gestionados dentro del componente de planificación del MSPI.

La siguiente ilustración muestra los niveles de madurez y el grado de cumplimiento de cada uno de estos, en la universidad:

Ilustración 2. Nivel de cumplimiento frente a la implementación del MSPI
Fuente: Adaptada para la Universidad del Quindío

A continuación, se puede observar el resultado del nivel de madurez de acuerdo con los objetivos de control de los dominios del Anexo A de la Norma ISO/IEC 27001:2013.



Gráfica 2. Porcentaje de cumplimiento de los dominios Anexo A de la Norma ISO/IEC 27001:2013
Fuente: Propia - Universidad del Quindío

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	**INICIAL**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	12	100	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	36	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	28	100	**REPETIBLE**
A.9	CONTROL DE ACCESO	39	100	**REPETIBLE**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	58	100	**EFECTIVO**
A.12	SEGURIDAD DE LAS OPERACIONES	56	100	**EFECTIVO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	78	100	**GESTIONADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	58	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	60	100	**EFECTIVO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	43	100	**EFECTIVO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	34	100	**REPETIBLE**
A.18	CUMPLIMIENTO	25	100	**REPETIBLE**
PROMEDIO EVALUACIÓN DE CONTROLES		**39**	**100**	**REPETIBLE**

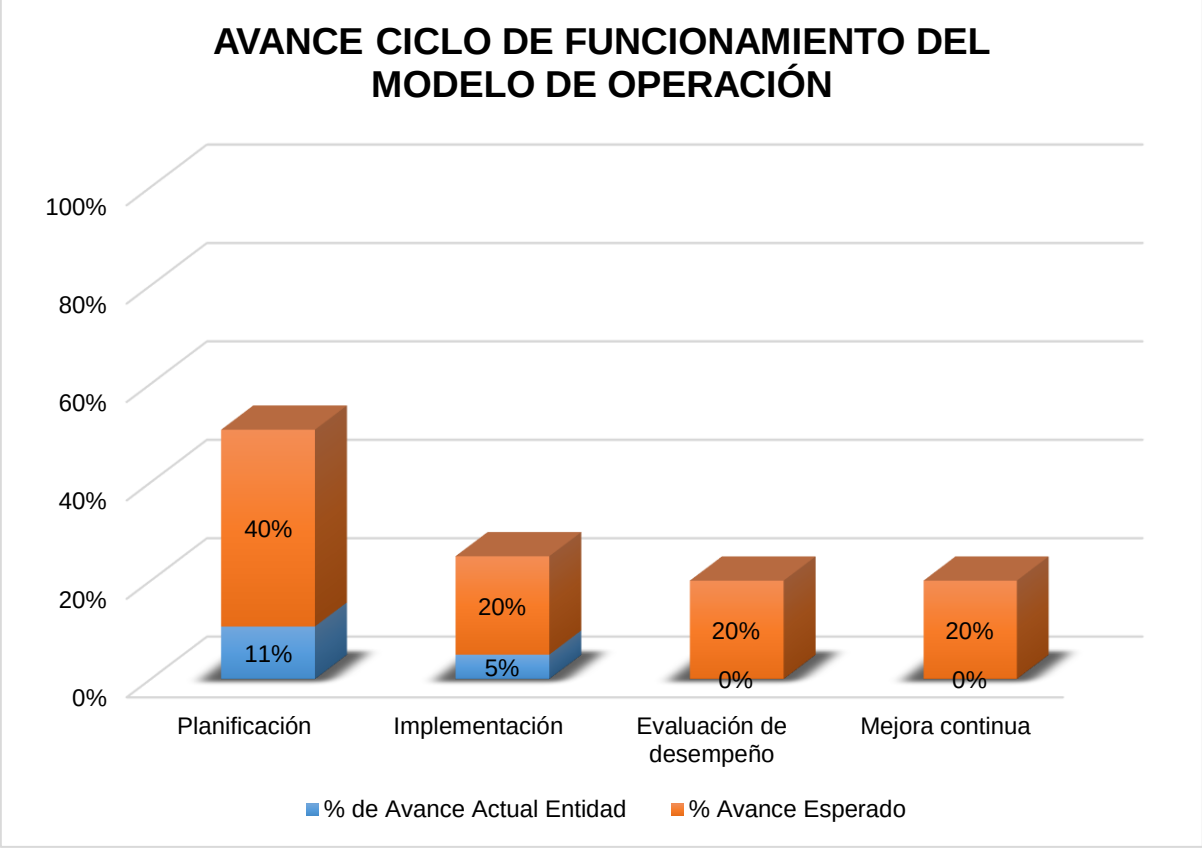
Tabla 1. Resultados de la evaluación del Anexo A de la Norma ISO/IEC 27001:2013
Fuente: Instrumento de diagnóstico GAP MinTIC aplicado en la universidad

El nivel de cumplimiento de los controles de seguridad de la información en la Universidad del Quindío con relación a los dominios de la norma ISO 27001:2013 alcanzó en nivel “EFECTIVO” en cinco (05) de estos, como se muestra a continuación, lo que evidencia que se ha logrado la estandarización, documentación y difusión de los controles.

- A.11; Seguridad física y del entorno
- A.12; Seguridad de las operaciones
- A.14; Adquisición, desarrollo y mantenimiento de sistemas
- A.15; Relaciones con los proveedores
- A.16; Gestión de incidentes de seguridad de la información

En lo que respecta al dominio de Seguridad en las Comunicaciones, se logró una efectividad del control como “GESTIONADO”; debido a que se tiene el servicio de SOC, que garantiza el monitoreo constante de los activos ante un posible ataque cibernético, configuraciones robustas a nivel del firewall, una arquitectura de red que permite la separación de la información crítica de la universidad, controles respecto a la segmentación de red, entre otros; como se puede evidenciar en el instrumento de análisis GAP, que hace parte integral de este documento.

Ahora bien, con respecto a la escala y niveles para establecer el cumplimiento del MSPI con el ciclo PHVA, en la siguiente imagen se observan los porcentajes para cada etapa y su nivel objetivo:



Gráfica 3. Resultados de avance del MSPI frente al PHVA
Fuente: Instrumento de diagnóstico GAP MinTIC aplicado en la universidad

Año	AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)		
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
2022	Planificación	11%	40%
	Implementación	5%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		**16%**	**100%**

Tabla 2- Resultados de avance del MSPI frente al PHVA
Fuente: Instrumento de diagnóstico GAP MinTIC aplicado en la universidad

Respecto al punto de avance según el modelo de operación PHVA, la institución se sitúa en la fase de **Planificación con un 11% alcanzado**.

En la Universidad del Quindío, existen algunas políticas de seguridad de la información, indispensables para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, pero estas, se encuentran desactualizadas y no han sido socializadas a todas las partes interesadas, cuentan con controles de seguridad digital implementados desde la Dirección de TI y se implementan buenas prácticas de seguridad de la información, como se evidenció al evaluar cada uno de los dominios del Anexo A de la Norma ISO/IEC 27001:2013; sin embargo no se tienen documentados, no se implementa el monitoreo periódico y no se evalúan frecuentemente sus resultados para verificar su efectividad, que son actividades indispensables para la operación de un Sistema de Gestión.

En términos generales, en la universidad del Quindío existen lineamientos, procesos, políticas y controles básicos para la gestión de la seguridad y privacidad de la información, los cuales permiten gestionar riesgos e incidentes de seguridad de la información, sin embargo, estos no se encuentran enmarcados dentro de los componentes necesarios para la adopción del MSPI establecido por MinTIC.

5.2. FASE 2. PLANIFICACIÓN (EN EL CICLO PHVA: PLANEAR)

Posterior a la ejecución del Diagnóstico, se procede a desarrollar la fase de Planificación, la cual tiene como objetivo determinar las necesidades y objetivos de seguridad y privacidad de la información, el diseño de los instrumentos que permiten evidenciar la implementación de controles técnicos, planes de gestión de riesgos,

sensibilización, seguimiento y control, entre otros. Para esta fase, se debe tener en cuenta el mapa de procesos, el tamaño de la entidad y el contexto interno y externo.

Esta fase da el punto de partida para el proceso de implementación y puesta en marcha del SGSPI.

Para llevar a cabo esta fase, la universidad trabajará en los siguientes aspectos:

a) **Contexto:** Identificar el contexto de la universidad, permite determinar el alcance del SGSPI, los recursos a invertir, los procesos de implementación y despliegue, entre otros. Por lo que, haciendo uso de las directrices internas definidas por el Sistema Integrado de Gestión, se identificó el contexto interno y externo de la entidad, determinando la identificación de necesidades y expectativas de las partes interesadas frente a la seguridad de la información; lo que permitió definir como alcance para el SGSPI dos procesos de la universidad:

   - **Proceso Estratégico:** Gestión de Tecnologías de la Información
   - **Proceso Misional:** Docencia / Admisiones y Registro

b) **Liderazgo:** Determinar las funciones de seguridad y privacidad de la información, adoptando, implementando, manteniendo y mejorando continuamente el MSPI. En este aspecto, se realizó el diseño de la política General de Seguridad y Privacidad de la Información, se adopta el MSPI para la universidad y se definen los roles y responsabilidades frente a la seguridad de la información de todos los funcionarios y contratistas, así como las de los líderes y cada uno de los procesos que hacen parte activa para el mantenimiento del sistema de gestión.

   Sumado a lo anterior, se tiene presupuesto asignado para fortalecer la seguridad digital e implementar el SGSPI.

c) **Planeación**: En esta actividad se logró la identificación de activos de información e infraestructura crítica, para los procesos del alcance; así como la valoración de los riesgos de seguridad de la información y su respectivo plan tratamiento. de igual forma, se realizó el diseño de toda la documentación que compone el SGSPI con base en los controles establecidos en el Anexo A de la Norma ISO/IEC 27001:2013 (Procedimientos, formatos, guías, metodologías, planes y hojas de ruta para la adopción, revisión, seguimiento y monitoreo)

d) **Soporte:** Para lograr el desarrollo de las actividades de adopción del MSPI, la universidad contempla: determinar y proporcionar los recursos necesarios para su respectiva adopción. De igual forma, en esta actividad se contempla la definición de un plan de capacitación y sensibilización que permita a la Entidad contar con el conocimiento y formación necesario para la adopción del MSPI, la planificación de proyectos de inversión y los presupuestos para el mantenimiento del SGSPI en cada vigencia.

5.3. FASE 3. OPERACIÓN (EN EL CICLO PHVA: HACER)

Una vez se haya desarrollado la fase de planificación, la Entidad se dispondrá a realizar la implementación de los respectivos controles de seguridad que permitan la mitigación de los riesgos que se hayan identificado previamente. Para lograr el objetivo de esta fase, la universidad realizará la planificación e implementación del plan de tratamiento de riesgos de seguridad de la información que se haya construido en la Fase de Planificación. Es decir, en la fase de operación se implementan los planes y controles para lograr los objetivos del SGSPI. Dentro de las actividades de esta fase se contempla:

a) Implementar el Plan de Control y planeación Operacional.
b) Implementar el plan de Tratamiento de Riesgos de Seguridad y privacidad de la información.
c) Monitoreo de los indicadores de Seguridad de la Información.
d) Monitoreo y seguimiento a la implementación de controles de seguridad de la información.

5.4. FASE 4. EVALUACIÓN DE DESEMPEÑO (EN EL CICLO PHVA: VERIFICAR)

Una vez se haya terminado la fase de operación (implementación) se lleva a cabo la fase de Evaluación de desempeño, la cual permite a la universidad evaluar la efectividad de las acciones tomadas a través de los indicadores, monitoreo de riesgos e incidentes de seguridad de la información, de tal forma que permita evidenciar el nivel de efectividad del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI en la entidad. Dentro de esta fase se contemplan las siguientes actividades:

a) **Seguimiento, medición, análisis y evaluación.** En esta actividad la universidad garantizará que se conozca de manera permanente la gestión que se ha realizado para la adopción del MSPI, así como sus logros y metas. Esto requiere que se determinen los recursos para el monitoreo, el desempeño, los resultados y la aceptación formal por parte de la Entidad. Esta actividad

permite generar los resultados de los indicadores, así como los informes producto de la evaluación de desempeño.

b) **Auditoría Interna.** La universidad realizará auditorías Internas al MSPI (o SGSPI) de tal forma que permita identificar las debilidades y los controles a mejorar, así como el cumplimiento frente a la adopción del MSPI.

c) **Revisión por la dirección.** En esta actividad la universidad realizará el reporte respectivo de la información resultante de las evaluaciones de desempeño del MSPI, requerimientos de aprobación de documentos, incidentes, comportamientos y demás aspectos relevantes para que la dirección se encuentre al tanto y le permita determinar su conveniencia, adecuación y eficacia.

5.5. FASE 5. MEJORAMIENTO CONTINUO (EN EL CICLO PHVA: ACTUAR)

Como última fase del ciclo se lleva a cabo la fase de mejoramiento continuo, en la cual se establecen los compromisos, responsables y acciones necesarias para identificar y mitigar las desviaciones frente a la adopción efectiva del MSPI, así como las lecciones aprendidas en la implementación del SGSPI para su solución y no repetición. Es decir, se consolidan los resultados de la fase de evaluación de desempeño y se diseña el plan de mejoramiento continuo para adaptar oportunamente las condiciones e instrumentos que permitan a la entidad mitigar las debilidades que fueron encontradas en el proceso de operación y puesta en marcha del sistema de gestión. Como resultado de esta fase se debe actualizar el “Plan de Seguridad y Privacidad de la Información” así como la hoja de ruta o cronograma del plan operacional de seguridad de la información, o los respectivos planes correctivos o de mejoramiento, según lo indiquen los procedimientos internos de la universidad.

5.6. CRONOGRAMA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN)

Dentro de este cronograma se incluyen las actividades generales mencionadas dentro del presente documento y las fechas para su ejecución. De igual forma, la información detallada para llevar a cabo cada una de las fases descritas en este plan, se encuentran en la hoja llamada “Operacional”

Es importante aclarar que dependiendo de la madurez del SGSPI en la entidad frente a la adopción de MSPI, los cronogramas deben actualizarse cada año y según el contexto institucional, la adopción del sistema de gestión se realizará de manera gradual.

De igual forma, para la implementación del MSPI se seguirán las guías[3] y la documentación respectiva[4] dispuesta por el MinTIC, en materia de Seguridad de la Información, para las entidades del gobierno colombiano.

Actividades	2023		2024		2025	
	SEM1	SEM2	SEM1	SEM2	SEM1	SEM2
Diagnóstico del MSPI						
Identificación/Actualización del contexto						
Definición del alcance del MSPI						
Establecimiento del liderazgo						
Planeación						
Soporte y recursos						
Toma de conciencia-sensibilización						
Implementación de planes y controles.						
Seguimiento, medición, análisis y evaluación.						
Auditoría Interna						
Revisión por la dirección						
Plan de mejoramiento						

Tabla 3. Plan general de seguridad y privacidad de la Información.
Fuente: Propia – Universidad del Quindío

6. ANEXOS

Anexo 1. Cronograma del Plan Operacional de Seguridad y privacidad de la Información. (Dado que este anexo es de manejo interno de la universidad y será adaptado de acuerdo al contexto organizacional, no será objeto de publicación en la página web de la Entidad.)

[3] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
[4] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

DIRECCIÓN DE PLANEACIÓN INSTITUCIONAL

Tel: (57) 6 735 9300 Ext
Carrera 15 Calle 12 Norte
Armenia, Quindío – Colombia
sgsi@uniquindio.edu.co