UNIPAZ®
Instituto Universitario de la Paz

Plan de Seguridad y Privacidad de la Información

Oficina de Gestión TIC

2025

VIGILADA MINEDUCACIÓN

Tabla de Contenido

Lista De Figuras

Lista de Tablas

1. INTRODUCCIÓN

El uso de las tecnologías de la información y las comunicaciones, facilitan la creación de valor en las instituciones, pero es necesaria una adecuada selección e implementación de estas tecnologías, alineadas con la estrategia y la misión para tener éxito.

Desde el Instituto Universitario de la Paz - UNIPAZ, se conciben las tecnologías de la información y las comunicaciones como instrumentos fundamentales para lograr el cumplimiento de los planes y objetivos institucionales; resultado de esta intención de la alta dirección, es la inclusión de los procesos asociados a la gestión de tecnologías de información en los cuatro componentes que se abordan en el Plan de Desarrollo Institucional.

Las Tecnologías de la Información y las Comunicaciones-TIC hacen parte de la planificación estratégica que permite gestionar y gobernar de manera conjunta y alineada con la estrategia de toda la institución.

El Rector, lidera la planeación estratégica de las tecnologías de la información (TI) acorde con la estrategia (Misión-Visión), lo que le permitirá alcanzar las metas apuntando a la mejora continua y la eficacia de la gestión administrativa.

El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información del **INSTITUTO UNIVERSITARIO DE LA PAZ - UNIPAZ**, el cual, tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia, propuesto por la Política de Gobierno Digital y la norma ISO 27001:2013, los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad Digital y Privacidad de la Información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

2. OBJETIVOS

2.1. Objetivo General

Establecer un Plan de Privacidad y Seguridad de la Información que apoye la implementación del manual de Política de Seguridad Digital y Privacidad de UNIPAZ, acorde a los requerimientos del modelo de seguridad y privacidad de la información (MSPI) de la Política de Gobierno Digital, los requerimientos estratégicos de la institución y en cumplimiento de las disposiciones legales vigentes.

2.2. Objetivos Específicos

1. Definir las etapas del plan de seguridad de privacidad de la información del Instituto Universitario de la Paz - UNIPAZ, a partir del autodiagnóstico de la entidad, con el fin de establecer la estrategia de seguridad digital.
2. Implementar controles de seguridad y privacidad de la información en la vigencia 2025, mediante un cronograma que defina las actividades proyectadas.
3. Evaluar el nivel de implementación de la política de seguridad y privacidad de la información en el Instituto Universitario de la Paz - UNIPAZ en la vigencia 2025.

3. MARCO NORMATIVO

- Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
- Ley 23 de 1982. Sobre derechos de autor.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por 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 regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas.
- 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 prestan servicios públicos.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- 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 bases 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 de 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.
- Ley 1450 de 2011. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.
- 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.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 2088 de 2012. Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- 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 1753 de 2015. Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país.
- 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.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario.
- Decisión Andina 351 de 1993. Régimen común sobre derecho de autor y derechos conexos.
- Directiva 26 de 2020. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.
- 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 2609 de 2012. Por el 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 884 de 2012 Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- 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 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1068 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- 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 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el

modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.

- Decreto 1008 del 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 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 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- Decreto 1287 de 2020. Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Decreto 767 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.
- Decreto 88 de 2022. Por el cual se adiciona el Título 20 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 reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
- CONPES 3995 de 2020. Confianza y Seguridad Digital
- CONPES 3854 de 2017. Política Nacional de Seguridad digital.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 4069 de 2022. Política Nacional de Ciencia, tecnología e innovación 2022 – 2031.

4. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DIGITAL

4.1. Ciclo de Operación

En el presente capitulo se explica el ciclo de operación que el Instituto Universitario de la Paz - UNIPAZ implementará para el Modelo de Seguridad y Privacidad de la Información y de la Política de Seguridad Digital y Privacidad de la Información.

La metodología contempla, en su ciclo de operación cinco (5) etapas, las cuales permiten que el Instituto Universitario de la Paz - UNIPAZ pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información[1]

Esquema 1. Ciclo de Operación del Modelo de Seguridad Digital y Privacidad de la Información

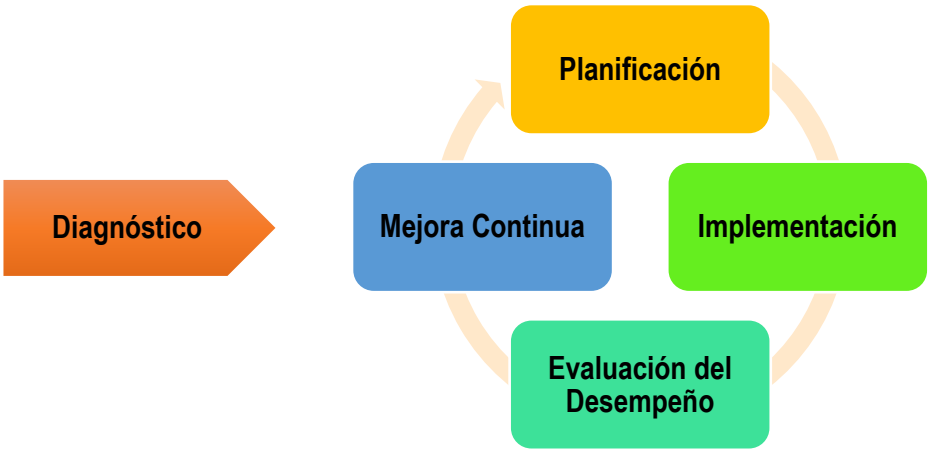

Figura No. 1 Ciclo de Operación del Modelo de Seguridad Digital. Fuente: Propia

Diagnóstico: Permite identificar el estado actual del Instituto Universitario de la Paz - UNIPAZ con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Planificación (Planear): En esta etapa se establecen los objetivos a alcanzar y las actividades del proceso a controlar mediante la implementación de políticas, así como los indicadores de medición para controlar y cuantificar los objetivos.

Implementación (Hacer): En esta etapa se ejecuta el plan establecido que consiste en realizar las acciones necesarias para lograr el cumplimiento de la política de seguridad digital y privacidad de la información.

Evaluación de desempeño (Verificar): Una vez implementada la política de seguridad digital y privacidad de la información, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones ejecutadas y su estado de cumplimiento.

Fase Mejora Continua (Actuar): Se analizan los resultados de las políticas implementadas y el nivel de incumplimiento de los objetivos definidos, con el fin de analizar las cusas de las desviaciones y generar los respectivos planes de mejora.

4.2. ALINEACIÓN NORMA ISO 27001:2013 VS CICLO DE OPERACIÓN

Debido a que la norma ISO 27001:2013 no determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de los modelos de gestión de la siguiente forma:

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Esquema 2. Alineación Norma ISO 27001:2013 con el Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información:

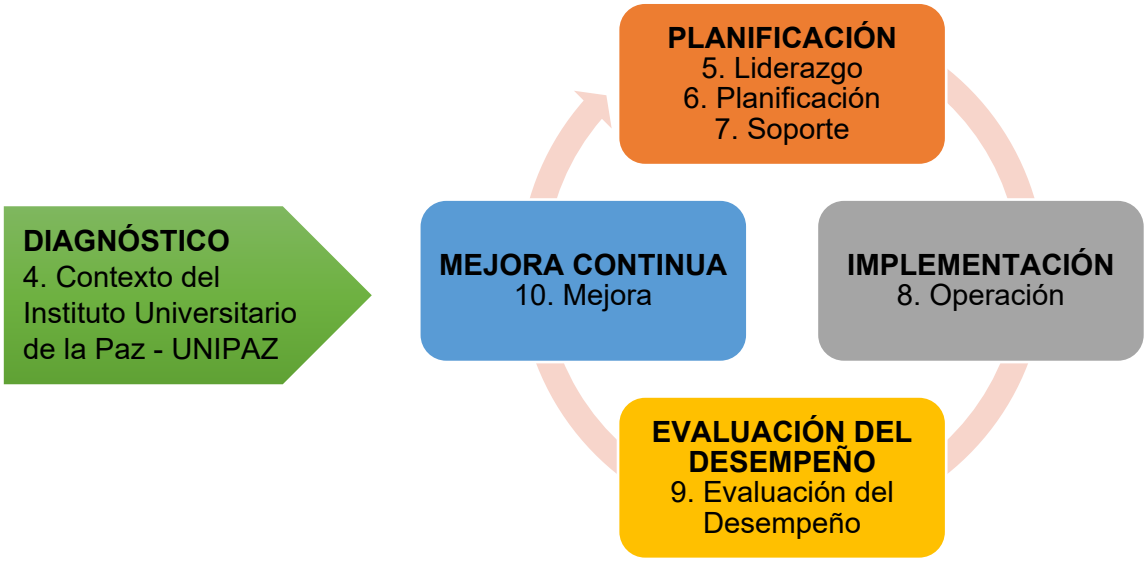

Figura No. 2 Alineación Norma ISO 27001:2013 Vs Ciclo de Operación del Modelo de Seguridad Digital. Fuente: Propia

Contextualización de las fases según la norma ISO 27001:2013:

- **Diagnóstico:** En el capítulo 4 **"Contexto de la organización"** de la norma, se determina la necesidad de realizar un análisis en el entorno externo e interno del Instituto Universitario de la Paz - UNIPAZ y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesadas de la Entidad en el alcance del SGSI.

- **Planeación**: En el capítulo 5 **"Liderazgo"**, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información (SGSI) y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito del Instituto Universitario de la Paz - UNIPAZ y asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

  En el capítulo 6 **"Planeación"**, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

  Finalmente, en el capítulo 7 **"Soporte"** se establecen los recursos necesarios para el establecimiento, implementación y mejora continua del SGSI.

- **Implementación**: En el capítulo 8 **"Operación"**, se indica que el Instituto Universitario de la Paz - UNIPAZ debe planificar, implementar y controlar los procesos necesarios para cumplir los

objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

- **Evaluación del Desempeño:** En el capítulo 9 **"Evaluación del desempeño"**, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del SGSI.

- **Mejora Continua:** En el capítulo 10 **"Mejora"**, se establece para el proceso de mejora del SGSI, que a partir de las no-conformidades que ocurran, el Instituto Universitario de la Paz - UNIPAZ debe establecer las acciones para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

4.3. Etapa I: Diagnóstico

Tabla 1 Descripción del Diagnóstico de MSPI

Objetivo	Identificar el estado del Instituto Universitario de la Paz - UNIPAZ con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información (MSPI) definidos en la Política de Gobierno Nacional.

Metas	Actividades / Instrumentos / Resultados
Determinar el **estado actual** de la gestión de seguridad digital y privacidad de la información al interior del Instituto Universitario de la Paz - UNIPAZ.	**Diagnostico** nivel de cumplimiento del Instituto Universitario de la Paz - UNIPAZ frente a los objetivos de control y controles establecidos en el **Anexo A** de la norma ISO 27001:2013. **Valoración** estado actual de la gestión de seguridad del Instituto Universitario de la Paz - UNIPAZ, con base en el **Instrumento de Evaluación MSPI de MINTIC**.
Identificar el **nivel de madurez** de seguridad digital y privacidad de la información.	Elaboración del documento **Nivel de Madurez** de seguridad y privacidad de la información, teniendo en cuenta las actividades anteriores de diagnóstico y contemplando lo propuesto en la guía "Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital" del Min. TIC.

Para la recolección de la información, en esta fase se utilizarán mecanismos como:

4. Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento del Instituto Universitario de la Paz - UNIPAZ, con relación a los dominios de la norma ISO/IEC 27001:2013.

5. Documentación existente en el Sistema Integrado de Gestión de Aseguramiento de la Calidad del Instituto Universitario de la Paz - UNIPAZ relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.

6. Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

4.4. Etapa II: Planificación

Esquema 3. Etapa de planificación del Modelo de seguridad digital y privacidad de la información

Figura No. 3 Etapa de Planificación del Modelo de Seguridad Digital. Fuente: Propia

Tabla 2 Descripción de la Planificación del MSPI

Objetivo	Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad digital y privacidad de la información, en procura de los resultados que permitan dar cumplimiento a la Política de Seguridad Digital y Privacidad de la Información.

Metas	Actividades / Instrumentos / Resultados
Realizar un análisis de contexto y factores externos e internos del Instituto Universitario de la Paz - UNIPAZ en torno a la seguridad de la información.	**Realizar** un **Análisis de Contexto** del Instituto Universitario de la Paz - UNIPAZ entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONTEXTO DE LA ORGANIZACIÓN de la norma ISO 27001:2013, con el fin de poder determinar las cuestiones externas e internas de la Entidad que son pertinentes para la implementación de la política de seguridad digital y privacidad de la información y la Política de administración del Riesgo en lo concerniente a la seguridad y privacidad de la información.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la	**Definir los roles y responsabilidades** para la implementación, administración, operación y gestión de la seguridad digital y

Metas	Actividades / Instrumentos / Resultados
información	privacidad de la información e incluirlos en el sistema integrado de calidad del Instituto Universitario de la Paz - UNIPAZ. **Definir** en la **estructura organizacional** del Instituto Universitario de la Paz - UNIPAZ la dirección y/o grupo a los que se le asignará los roles y responsabilidades pertinentes a la seguridad de la información. **Crear y/o Asignar el Rol de Oficial de Seguridad Digital** como responsable de la política de seguridad digital y privacidad de la información.
Definir la metodología de riesgos de seguridad de la información	**Definir la Metodología de Valoración de Riesgos de Seguridad Digital**. Integrar la metodología definida con la metodología de riegos, gestión y riesgos de corrupción del Instituto Universitario de la Paz - UNIPAZ.
Elaborar las políticas de seguridad digital y privacidad de la información del Instituto Universitario de la Paz - UNIPAZ y su plan de implementación.	**Elaborar** el **manual que incluya la política general y las Políticas de Seguridad Digital y Privacidad de la Información**, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en el Instituto Universitario de la Paz - UNIPAZ con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la entidad.
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de gestión de seguridad de la información.	**Elaborar** los documentos de operación del sistema de seguridad de la información, cómo mínimo los siguientes: ● Declaración de aplicabilidad. ● Procedimiento y/o guía de identificación y clasificación de activos de información. ● Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI. ● Procedimiento para control de documentos (SGSI). ● Procedimiento para la gestión de eventos e incidentes de seguridad de la información. ● Procedimiento para la gestión de vulnerabilidades de seguridad de la información.
Identificar y valorar activos de información	**Realizar la identificación y valoración de los activos de información** de la entidad de acuerdo con su nivel de criticidad y con el alcance del SGSI. **Documentar** el inventario de activos de información del Instituto Universitario de la Paz - UNIPAZ.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad	**Realizar la identificación y valoración de los riesgos transversales de seguridad de la información** y definir los respectivos planes de tratamiento. Realizar la valoración de riesgos de seguridad de la información de acuerdo con el alcance del SGSI. **Definir los planes de acción** que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos.

Metas	Actividades / Instrumentos / Resultados
	Para la selección de los controles, se tomará como base los objetivos de control y los controles establecidos en el **Anexo A** de la norma ISO/IEC 27001:2013
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información	**Elaborar** plan anual de capacitación y sensibilización anual de seguridad digital y privacidad de la información.

4.5. Etapa III: Implementación

Esquema 4. Etapa de implementación del modelo de seguridad digital y privacidad de la información.

Figura No. 4 Etapa de Implementación del Modelo de Seguridad Digital. Fuente: Propia

Tabla 3 Descripción de la Etapa de Implementación del MSPI

Objetivo	Llevar a cabo la implementación de cada una de las actividades planificadas en la etapa II, para dar cumplimiento a la Política de Seguridad Digital y Privacidad de la Información

Metas	Actividades / Instrumentos / Resultados
Ejecutar el plan de tratamiento de riesgos	**Ejecutar el plan de tratamiento de los riesgos transversales** de seguridad de la información
Establecer indicadores de gestión de seguridad digital.	**Definir los indicadores** para medir la gestión del modelo de seguridad digital y **establecer** los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad digital del Instituto Universitario de la Paz - UNIPAZ.
Implementar procedimiento de gestión de eventos e incidentes de seguridad digital.	**Implementar** el procedimiento y los mecanismos para la **gestión de los eventos e incidentes de seguridad de la información.**
Implementar procedimiento de gestión de vulnerabilidades.	**Implementar** el procedimiento y los mecanismos para la gestión de vulnerabilidades seguridad de la información.
Ejecutar plan de capacitación y sensibilización de seguridad digital y privacidad de la información.	**Ejecutar** el plan anual de capacitación, socialización y sensibilización de seguridad digital y privacidad de la información.
Ejecutar pruebas anuales de vulnerabilidades e intrusión	**Ejecutar** el plan anual de pruebas vulnerabilidades e intrusión con el objetivo de **identificar el nivel de protección de los activos de información** del Instituto Universitario de la Paz - UNIPAZ.

4.6. Fase IV: Evaluación y Desempeño

Esquema 5. Etapa de evaluación y desempeño del modelo de seguridad

Figura No. 5 Etapa de evaluación y Desempeño del Modelo de Seguridad Digital. Fuente: Propia

Tabla 4 Descripción de la Etapa de Evaluación y Desempeño del MSPI.

Objetivo	Evaluar el desempeño y la eficacia del Modelo de Seguridad y Privacidad de la información, a través de instrumentos que permitan determinar la efectividad de la implementación de la Política de Seguridad Digital y Privacidad de la Información.

Metas	Actividades / Instrumentos / Resultados
Ejecución de auditorías de seguridad de la información.	Ejecución de auditorías del modelo de gestión de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables al Instituto Universitario de la Paz - UNIPAZ, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección. Las auditorías internas se deberán llevar a cabo para la revisión del Sistema de Gestión de Seguridad 'SGSI' de la Información implementado en el Instituto Universitario de la Paz - UNIPAZ, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumpla con los requisitos establecidos en la norma ISO 27001:2013 y los del MSPI.
Plan de seguimiento, evaluación y análisis de SGSI.	Elaboración documento con el plan de seguimiento, evaluación y análisis del SGSI revisado y aprobado por el Comité Institucional de Gestión y Desempeño.

4.7. Fase V: Mejora Continua

Esquema 6. Etapa de mejora continua del Modelo de Seguridad.

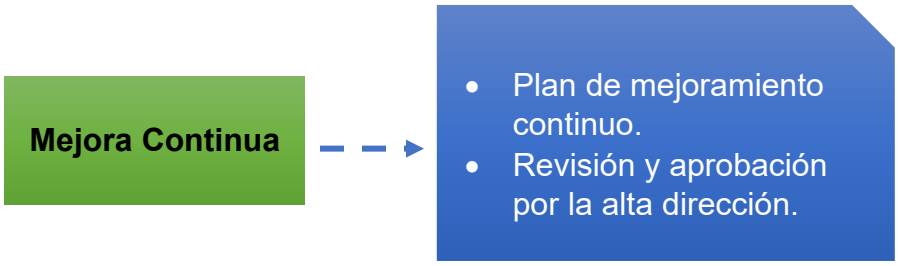

Figura No. 6 Etapa de Mejora Continua del Modelo de Seguridad Digital. Fuente: Propia

Tabla 5 Descripción de la Etapa de Mejora Continua

Objetivo	Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad digital y privacidad de la información, que permita realizar el plan de implementación de las acciones de mejora identificadas para el SGSI

Metas	Actividades / Instrumentos / Resultados
Diseñar plan de mejoramiento de Seguridad Digital y Privacidad de la Información	Diseñar el plan de mejoramiento continuo de seguridad digital y privacidad de la información, que permita realizar el plan de implementación de las acciones de mejora identificadas para el Sistema de Gestión de Seguridad de la Información

4.8. Cronograma del Plan de Implementación de Seguridad Digital y Privacidad de la Información

El presente documento, presenta una actualización al desarrollo de las actividades de implementación, con miras de establecer una propuesta de diseño del Modelo de Seguridad y Privacidad de la Información –

ACTIVIDAD	RESPONSABLE											
	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Elaboración del manual de políticas de seguridad y privacidad de la información												
Realizar el autodiagnóstico de la política de seguridad y privacidad de la información												
Identificar el nivel de madurez relacionado con la seguridad y privacidad de la información												
Matriz de verificación de requisitos legales de seguridad de la información												
Diseñar el procedimiento de gestión de incidentes de seguridad y privacidad de la información												
Elaborar el plan de continuidad de negocio												
Gestionar los incidentes y/o ataques con su respectiva documentación												
Diseña y ejecutar un plan de cambio y cultura de seguridad y privacidad de la información												
Implementación de controles de seguridad digital y privacidad de la información												
Auditoría interna de seguridad y privacidad de la información												
Propuesta de diseño del modelo de seguridad y privacidad de la información												