UNIVERSIDAD DE CUNDINAMARCA

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FUSAGASUGÁ
2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) de la Universidad de Cundinamarca se diseña como un instrumento clave de gobernanza institucional, alineado con el Plan Estratégico de Tecnologías de la Información (PETI) 2024–2027, como con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Este plan responde a la necesidad de consolidar una estrategia de protección de la información que esté en plena conformidad con los requisitos de la norma ISO/IEC 27001:2022, a su vez, da cumplimiento a la normativa colombiana vigente en materia de protección de datos personales, transparencia, y gobierno digital.

En este contexto, la Universidad de Cundinamarca establece una hoja de ruta que prioriza la implementación de controles estratégicos y técnicos que garanticen la confidencialidad, integridad y disponibilidad de la información en todos los niveles académicos y administrativos. El PESI se estructura conforme al ciclo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar), articulando sus ejes con los proyectos y metas trazadas en el PETI institucional.

Este plan refleja el compromiso institucional con la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) robusto, resiliente y orientado a la prevención de riesgos, apoyado además por un Programa Integral de Gestión de Datos Personales, asegurando así la protección de los derechos de los titulares de la información y el cumplimiento del marco normativo nacional e internacional aplicable.

2. OBJETIVOS:

2.1 OBJETIVO GENERAL

Establecer e implementar el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) como marco de acción institucional para salvaguardar la confidencialidad, integridad, disponibilidad de los activos de la información de la Universidad de Cundinamarca, a partir de la implementación de estrategias de seguridad, privacidad y ciberseguridad de la información, conforme a la norma ISO/IEC 27001:2022, el MSPI del MinTIC y el Plan Estratégico de Tecnologías de la Información (PETI).

2.2 OBJETIVO ESPECÍFICOS

- Establecer las etapas estratégicas para diseñar, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información - SGSI, conforme a la norma ISO/IEC 27001:2022.
- Definir y establecer las necesidades de la institución en materia de seguridad, privacidad y ciberseguridad, en el marco de los objetivos del PETI y la transformación digital.
- Identificar, clasificar y priorizar los proyectos de seguridad de la información, asegurando su alineación con los objetivos institucionales y la gestión de riesgos tecnológicos.
- Planificar mecanismos de evaluación, seguimiento y mejora continua de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información, incluyendo indicadores de desempeño, auditorías internas y revisión por la dirección.
- Establecer la línea base de madurez en seguridad de la información que permita la adopción progresiva del MSPI en todos los procesos institucionales y certificar a largo plazo el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) basado en la Norma ISO/IEC 27001 y los lineamientos definidos por MinTIC.
- Garantizar el cumplimiento de 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 y privacidad de la información.
- Fomentar una cultura institucional de ciberseguridad y corresponsabilidad, involucrando a todas las partes interesadas en la implementación y mejora del SGSI.

3. ALCANCE:

El presente documento establece el marco de acción institucional para implementar, de forma progresiva y estructurada, el Sistema de Gestión de Seguridad de la Información (SGSI) y el Programa Integral de Gestión de Datos Personales, conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), la Estrategia de Gobierno Digital y la norma ISO/IEC 27001:2022.

El alcance del PESI abarca:

- Todos los procesos académicos, administrativos, tecnológicos y de soporte de la Universidad de Cundinamarca.

- Todas las sedes, seccionales, extensiones, oficina de Bogotá, Centro Académico Deportivo – CAD y unidades agroambientales que procesen o custodien información institucional o datos personales.

- Todos los activos de información, incluyendo personas, procesos, tecnologías, infraestructura, servicios en la nube y proveedores estratégicos.

La ejecución de las actividades se desarrolla en vigencias anuales, con base en un cronograma articulado al PETI y sujeto a la disponibilidad presupuestal del Banco de Proyectos Institucional, priorizando iniciativas estratégicas, de cumplimiento normativo y de mitigación de riesgos. El seguimiento y evaluación del avance del PESI se realiza de forma periódica en la Comisión de Gestión, garantizando su alineación con los objetivos institucionales y el compromiso continuo con la mejora del SGSI y la protección de la información.

4. DEFINICIONES

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

- **ACTIVO DE INFORMACIÓN**: Se refiere a cualquier información o elemento en físico y/o digital para el procesamiento, almacenamiento, comunicaciones, procesos, procedimientos y recursos humanos asociados con el manejo y uso de los datos para llevar a cabo las actividades estratégicas, misionales, de apoyo y seguimiento de la institución.[1]

- **CONFIDENCIALIDAD**: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados según sea requerida.[2]

- **DISPONIBILIDAD**: Propiedad de la información de estar accesible y utilizable, cuando lo requiera una entidad autorizada.[3]

- **CONTROL:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **INTEGRIDAD**: Propiedad de la información relativa a su exactitud y completitud.[4]

- **RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.[5]

- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital.[6]

---

1 DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional De Política Económica y Social República De Colombia, CONPES 3854 de 2016 [sitio web]. Bogotá D.C. [Consultado: 25 de octubre de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

2 INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Requisitos. ISO/IEC 27001. Bogotá D.C.: El Instituto, 2014. 30 p

3 INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión de Incidentes de Seguridad de la Información, Conceptos Básicos. ISO/IEC 27035. Bogotá D.C.: El Instituto, 2014. 2 p

4 Ibidem

5 INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Definiciones. ISO/IEC 27000. Bogotá D.C.: El Instituto, 2014. 7 p

6 Ibidem

5. NORMATIVIDAD

La normatividad externa como son Constitución, leyes, decretos, resoluciones y demás, se encuentran documentadas en el **AJUr011** – MATRIZ DE IDENTIFICACIÓN Y SEGUIMIENTO AL CUMPLIMIENTO DE REQUISITOS LEGALES Y OTROS, atendiendo los lineamientos establecidos en el procedimiento **AJUP08** – IDENTIFICACIÓN, ACTUALIZACIÓN, SEGUIMIENTO AL CUMPLIMIENTO DE REQUISITOS LEGALES Y OTROS.

El documento **AJUr011** de la Dirección Jurídica, se encuentra publicado, en el Modelo de Operación Digital, en el Macroproceso Apoyo, Proceso Gestión Jurídica en el enlace: https://www.ucundinamarca.edu.co/sgc/index.php/macroproceso-apoyo/proceso-gestion-juridica

6. GOBIERNO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Universidad de Cundinamarca, atendiendo la normatividad y lineamientos establecidos en el *Modelo de Seguridad Y Privacidad de la Información - (MSPI) del* Ministerio de Tecnologías de la Información y las Comunicaciones abril 2025 y en alineación con las disposiciones de la norma ISO/IEC 27001:2022, ha establecido una estructura de gobernanza institucional de seguridad de la información que garantiza liderazgo, autoridad, rendición de cuentas y articulación con otros sistemas de gestión.

En este marco, la Universidad ha expedido y adoptado el siguiente conjunto normativo y organizacional:

De conformidad con Roles y responsabilidades, la institución mediante Resolución 144 de 2025 “POR EL CUAL SE DESIGNA AL COORDINADOR DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD DE CUNDINAMARCA”., con el fin de poder realizar la labor de implementación del SGSI de manera eficiente e integrar la Ciberseguridad como un pilar fundamental, se hace necesario designar un coordinador del Sistema de Gestión de Seguridad de la Información – SGSI, Ciberseguridad y la Protección de Datos Personales de los Titulares de la Universidad de Cundinamarca.

Atendiendo el compromiso de ***Liderazgo y Compromiso***, la institución mediante Resolución 088 de 2023 *“POR LA CUAL SE ESTABLECE EL SISTEMA DE ASEGURAMIENTO DE LA CALIDAD DE LA UNIVERSIDAD DE CUNDINAMARCA”*, documento que evidencia la participación de la Coordinador(a) del Sistema de Gestión de Seguridad de la Información – SGSI con voz y voto en la Comisión de Gestión *ARTÍCULO TRIGÉSIMO SEXTO. – COMISIÓN DE GESTIÓN* y con voz en la Comisión de Control Interno *ARTÍCULO CUADRAGÉSIMO. – COMISIÓN DE CONTROL INTERNO.*

De igual manera, atendiendo el ítem de ***Política de seguridad y privacidad de la***

información, la institución emitió las Resoluciones *No. 091 del 2023 "POR LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA y No. 092 del 2023 "POR LA CUAL ADOPTA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI Y SE ESTABLECEN LINEAMIENTOS, OBJETIVOS Y ALCANCE, EN LA UNIVERSIDAD DE CUNDINAMARCA".*

Todos estos lineamientos y disposiciones han sido consolidados y estructurados dentro del Manual ESG-SSI-M001 - Manual de Políticas de Seguridad y Privacidad de la Información, el cual establece el marco normativo y operativo del SGSI, incluyendo políticas, responsabilidades, y mecanismos de revisión, en cumplimiento de los controles A.5.1 a A.5.5 de la ISO/IEC 27002:2022. Esta estructura de gobierno garantiza que el SGSI opere con liderazgo, integridad, trazabilidad y mejora continua, permitiendo una gestión efectiva de los riesgos de seguridad y privacidad a nivel institucional.

6.1 ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Como parte integral del diseño, implementación, operación y mejora continua del SGSI, la Universidad de Cundinamarca, ha establecido una estructura clara de roles y responsabilidades, con el fin de asegurar la efectiva aplicación de las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) y de la norma ISO/IEC 27001:2022 en todos los niveles y procesos institucionales. La asignación de responsabilidades permite garantizar que los controles de seguridad y privacidad se implementen de forma sistemática y coherente en las áreas académicas, administrativas, operativas y tecnológicas, monitoreando su cumplimiento y tomando las acciones necesarias para reducir riesgos y prevenir incidentes.

Con este propósito, la Universidad ha adoptado el documento **ESG-SSI-M004** MANUAL DE ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, el cual contiene los distintos roles y responsabilidades en Seguridad y Privacidad de la Información, que son asignados a cada funcionario administrativo dentro de las distintas sedes, seccionales y extensiones, oficina de Bogotá, granjas agroambientales y el Centro Académico Deportivo – CAD, al momento de vincularse con la institución, sin importar su tipo de contratación; y que, por tanto, representan las directrices de necesario y obligatorio cumplimiento, al momento de recolectar, almacenar, circular, modificar o eliminar datos personales de Titulares e información reservada o confidencial de la Institución, a fin de reducir el riesgo de materialización de un incidente de seguridad y privacidad de la información.

7. METODOLOGÍA E IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI

7.1 FASES DE IMPLEMENTACIÓN

El Modelo de Seguridad y Privacidad de la Información dentro de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

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

- Fase Diagnostico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

- Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

- Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

- Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se

establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

- Fase Mejora Continua (Actuar): Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

7.2 FASES DEL CICLO OPERATIVO.

7.2.1 FASE I: DIAGNOSTICO - ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

De acuerdo con el análisis GAP del Modelo de Seguridad y Privacidad de la Información, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2022 es del **71%**, como se detalla en el siguiente gráfico.

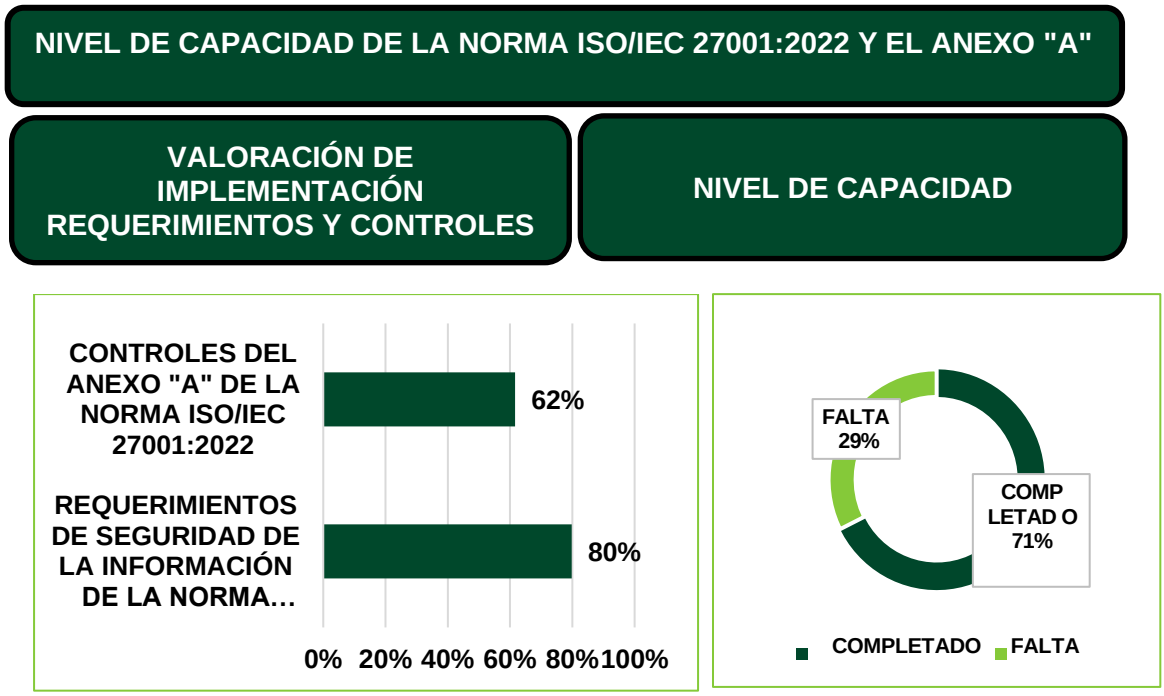

Ilustración 2. Análisis GAP del SGSI
Fuente: Propia - Universidad del Cundinamarca

Este avance se distribuye en dos secciones principales:

Requisitos de la ISO 27001:2022: El nivel de implementación en relación con los requisitos específicos de la norma es del **80%**, como se detalla en el siguiente gráfico.

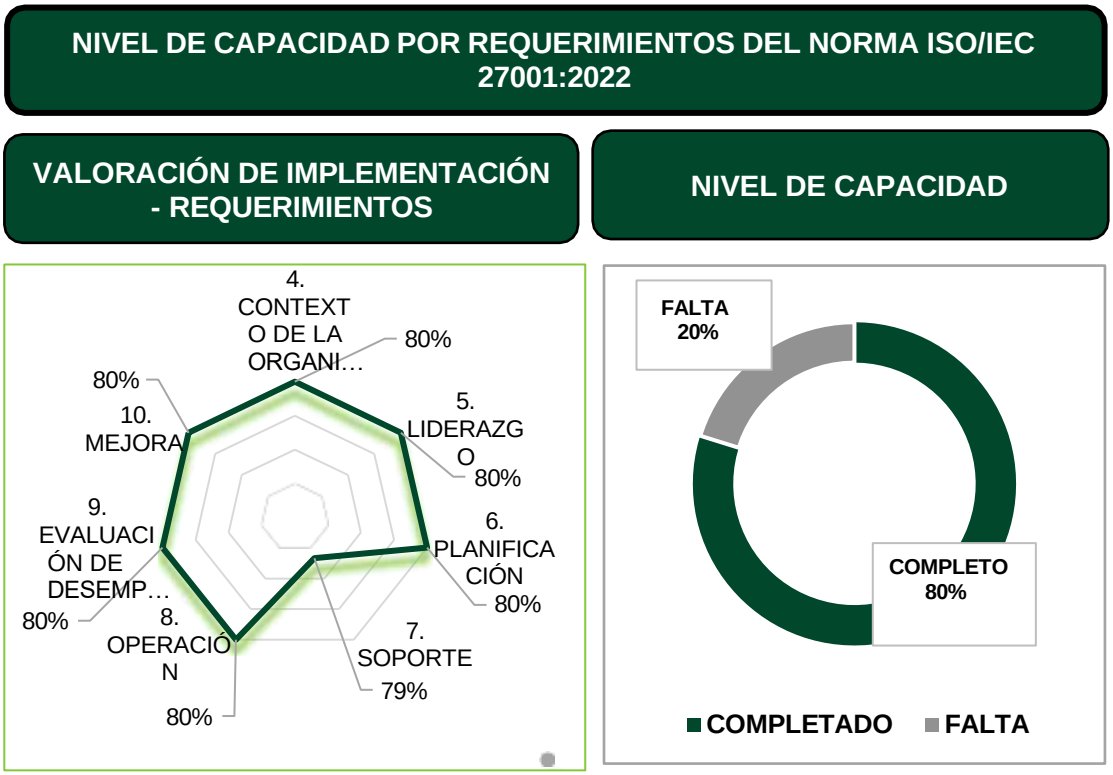

Ilustración 3. Análisis GAP del SGSI
Fuente: Propia - Universidad del Cundinamarca

Controles del Anexo A de la ISO 27001:2022: En cuanto al nivel de implementación de los controles categorizados en Organizacionales, de Personas, Físicos y Tecnológicos, el nivel actual es del **62%**, evidenciando áreas de oportunidad que deben ser abordadas para cumplir plenamente con la norma.

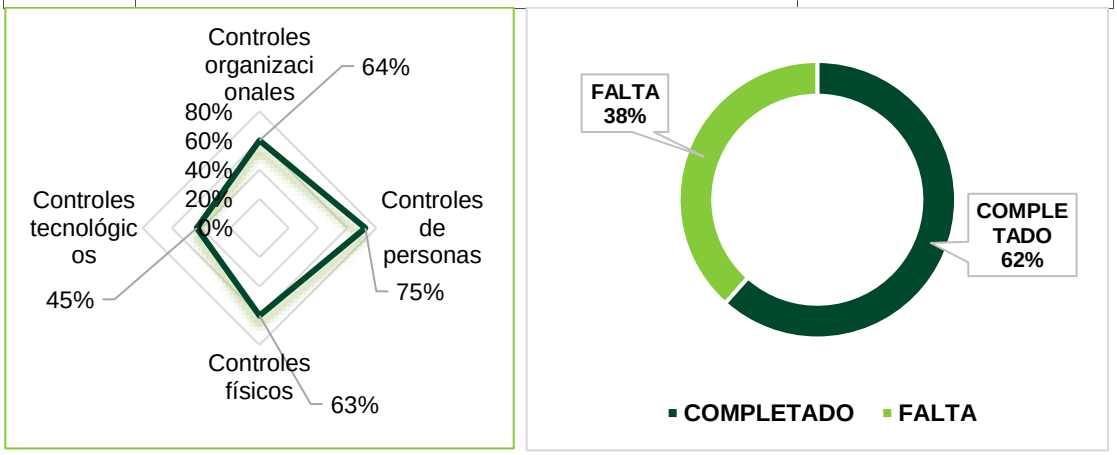

Ilustración 4. Análisis GAP del SGSI
Fuente: Propia - Universidad del Cundinamarca

Esto de acuerdo con la escala de valoración dada por el Min Tic frente a las cuatro (4) categorías (Organizacionales, de personas, Físicos y Tecnológicos) evaluadas, se identificó que la Universidad de Cundinamarca, tiene un cumplimiento general del MSPI del **71%** encontrándose en un nivel de madurez "**Grado de Cumplimiento**", lo que indica que "*Los procesos y los controles se documentan y se comunican. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada*".

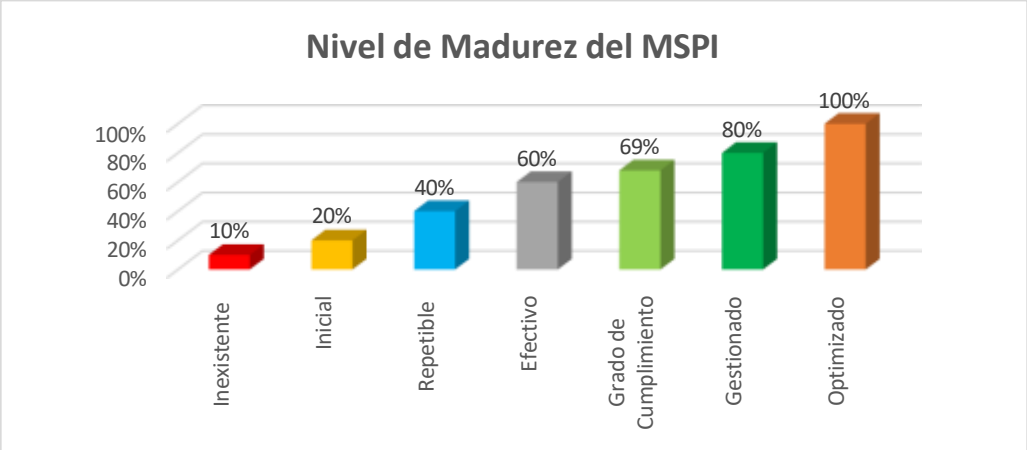

Ilustración 5. Niveles de madurez frente a la implementación del MSPI
Fuente: Propia - Universidad del Cundinamarca

La siguiente ilustración muestra los niveles de madurez y el grado de cumplimiento de cada una de las categorías de controles del anexo A de la Norma ISO 27001:2022, en la universidad:

Evaluación de Efectividad de Control			
Categoría	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de Efectividad de Control - MSPI**
A.5 Controles Organizacionales	64%	100%	Efectivo
A.6 Controles De Personas	75%	100%	Efectivo
A.7 Controles Físicos	63%	100%	Efectivo
A.8 Controles Tecnológicos	45%	100%	Repetible
Promedio evaluación de Controles	**62%**	**100%**	**Efectivo**

Tabla 1. Resultados de la evaluación del Anexo A de la Norma ISO/IEC 27001:2013 Vs MSPI
Fuente: Análisis GAP aplicado en la universidad

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

Con base en los resultados del diagnóstico de brechas del SGSI y en alineación con los requisitos de la norma ISO/IEC 27001:2022, la Universidad de Cundinamarca procede a desarrollar la fase de Planificación, como punto de partida estratégico para establecer el marco de gestión de seguridad y privacidad de la información. Esta fase permite determinar las necesidades y objetivos de seguridad y privacidad de la información, el diseño de los instrumentos que permitan 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.

Para llevar a cabo esta fase, la Universidad de Cundinamarca trabajará en los siguientes aspectos:

a) Contexto: En este caso, se determinó los elementos externos e internos que son relevantes con las actividades que realiza la institución en el desarrollo de su misión y las partes interesadas internas o externas y personas, entidades u organizaciones que pueden influir directamente en la seguridad y privacidad de la información, esto con el propósito de determinar los límites y la aplicabilidad del MSPI en el marco del modelo de operación por proceso de la Universidad de Cundinamarca.

b) Liderazgo: En este aspecto, se formalizo la política General de Seguridad y Privacidad de la Información, se adopta el MSPI como marco de referencia institucional para la Universidad de Cundinamarca y se definen los roles y

responsabilidades específicos frente a la seguridad de la información de todos los funcionarios y contratistas, así como las de los líderes de los procesos que hacen parte activa para el mantenimiento del Sistema de Gestión de Seguridad de la Información. Así mismo la alta dirección garantiza la asignación de recursos financieros, humanos y tecnológicos, alineados al Banco de Proyectos, para asegurar la implementación efectiva del SGSI.

c) Planeación: En este caso se logró la identificación de activos de información e infraestructura crítica, para los procesos dentro del alcance; así como la valoración de los riesgos de seguridad de la información y su respectivo plan tratamiento, de igual manera, se diseñó la documentación que soporta el SGSI con base en los controles establecidos en el Anexo A de la Norma ISO/IEC 27001:2022 (Procedimientos, manuales, formatos, guías, instructivos).

d) Soporte: Para lograr el desarrollo de las actividades de adopción del MSPI, la Universidad de Cundinamarca contempla: determinar y proporcionar los recursos necesarios para su respectiva adopción. De igual forma, en esta actividad se contempla la definición del plan de capacitación y sensibilización que permita a la institución asegurar la competencia del personal frente a las responsabilidades de seguridad necesarias para la adopción del MSPI, la planificación de proyectos de inversión y los presupuestos para el mantenimiento del SGSI en cada vigencia.

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

Una vez se haya desarrollado la fase de planificación, la Universidad de Cundinamarca 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 ejecutar los planes de tratamiento de riesgos de seguridad de la información que se haya construido en la Fase de Planificación, con el objetivo de proteger los activos de información de la Universidad frente a amenazas internas y externas, reduciendo los riesgos a niveles aceptables para la organización. Es decir, en esta fase se implementan los planes y controles de seguridad para lograr los objetivos del SGSI. Dentro de las actividades de esta fase se contempla:

a) Implementar el plan Operacional de Seguridad de la información.
b) Ejecución del plan de Tratamiento de Riesgos de Seguridad y privacidad de la información conforme a los resultados del análisis y valoración.
c) Monitoreo de los indicadores de Seguridad de la Información, para validar la eficacia de las medidas adoptadas.
d) Monitoreo y seguimiento a la implementación de controles de seguridad de la información, asegurando trazabilidad y ajuste ante desviaciones.

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

Esta fase permite a la Universidad de Cundinamarca evaluar la efectividad de las acciones tomadas a través de métodos formales y periódicos de verificación, como indicadores, monitoreo de riesgos e incidentes de seguridad de la información, asegurando que los objetivos del SGSI están siendo alcanzados de manera eficaz y conforme a las expectativas institucionales. Dentro de esta fase se contemplan las siguientes actividades:

a) Seguimiento, medición, análisis y evaluación del SGSI, incluyendo el cumplimiento de metas del PESI, ejecución de proyectos, y monitoreo de riesgos e incidentes, garantizando que se conozca de manera permanente la gestión que se ha realizado para la adopción del MSPI.
b) Auditorías Internas al Sistema de Gestión de Seguridad de la información SGSI bajo estándares como ISO/IEC 27001, de tal forma que permita identificar las debilidades y oportunidades de mejora, garantizando el cumplimiento del MSPI.
c) Revisión por la dirección mediante el reporte consolidado de la información resultante de las evaluaciones de desempeño del MSPI, incidentes, comportamientos y demás aspectos relevantes que afecten al SGSI, con el fin de que la alta dirección se encuentre al tanto y le permita determinar su conveniencia, adecuación y eficacia.

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

Como última fase del ciclo la mejora continua es un principio rector del SGSI y una exigencia formal de la ISO/IEC 27001:2022. En esta fase, la Universidad de Cundinamarca define las acciones correctivas, preventivas y de mejora derivadas de auditorías, análisis de incidentes, revisiones directivas y lecciones aprendidas en la implementación del SGSI. Como resultado de esta fase se debe actualizar el “Plan Estratégico de Seguridad y Privacidad de la Información - PESI” así como el cronograma del Plan operacional de seguridad de la información, y los respectivos planes correctivos o de mejoramiento, según lo indiquen los procedimientos internos de la institución.

7.7 ALINEACIÓN NORMA ISO 27001:2022 VS CICLO DE OPERACIÓN.

El Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad de Cundinamarca se estructura conforme al principio de mejora continua, utilizando el modelo PHVA (Planear, Hacer, Verificar, Actuar) como eje metodológico. Este enfoque asegura una gestión dinámica, iterativa y basada en riesgos, alineada con los requisitos de la norma ISO/IEC 27001:2022 y los lineamientos del Modelo de

Seguridad y Privacidad de la Información (MSPI), por lo cual a continuación se muestra la alineación de la norma y el ciclo operativo:

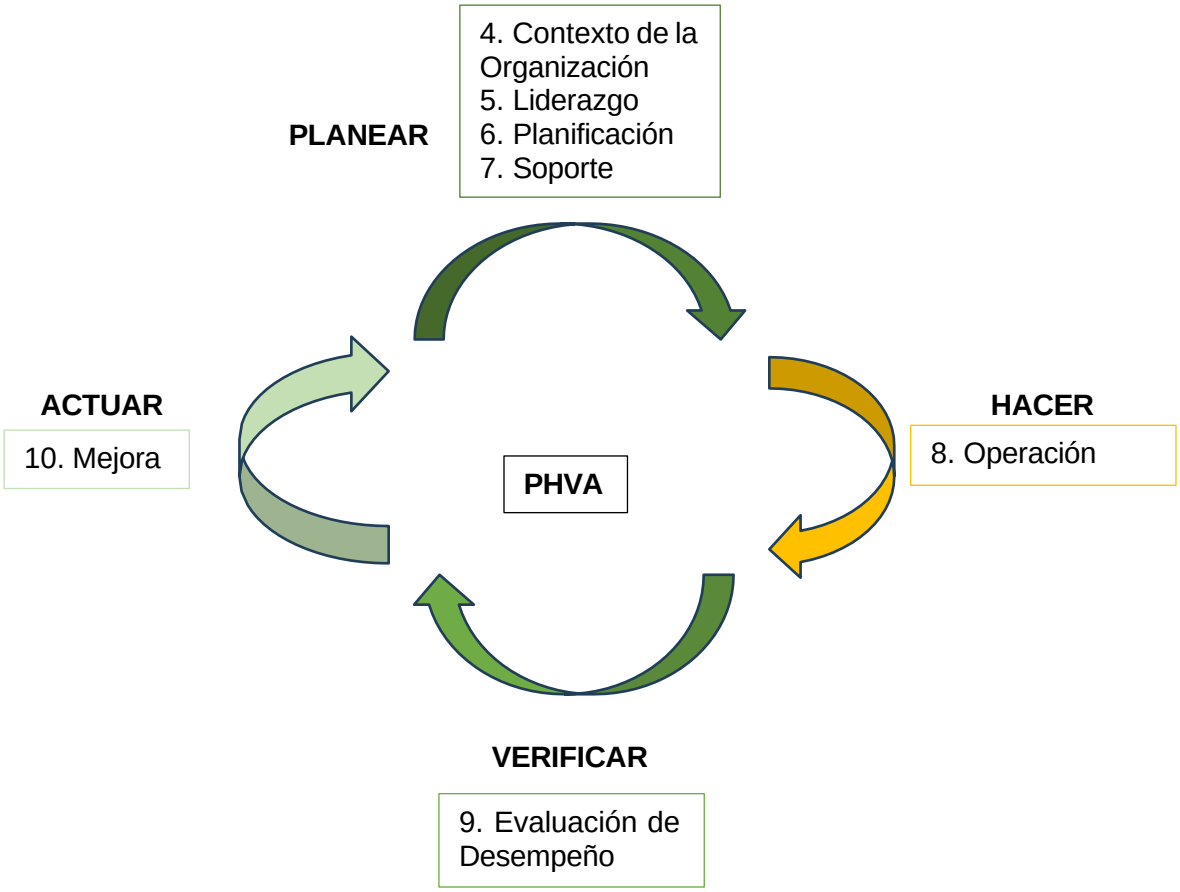

Ilustración 6. Fases de la implementación del MSPI
Fuente: Propia - Universidad del Cundinamarca

Ciclo PHVA	***Cláusulas ISO/IEC 27001:2022***	***Descripción***
Planear	*4 – Contexto de la organización* *5 – Liderazgo* *6 – Planificación*	*Define el propósito, alcance, requisitos, liderazgo, roles, evaluación de riesgos, objetivos y planificación del SGSI.*
Hacer	*7 – Apoyo* *8 – Operación*	*Se implementan los controles, recursos, competencias, concienciación y procesos necesarios para gestionar los riesgos y alcanzar los objetivos del SGSI.*
Verificar	*9 – Evaluación del desempeño*	*Se realiza el seguimiento, medición, auditoría interna y revisión por la dirección para determinar la eficacia del sistema.*

Actuar	*10 – Mejora*	*Se identifican no conformidades, se establecen acciones correctivas y se mejoran continuamente los procesos del SGSI.*

Tabla 2 Alineación del ciclo operativo PHVA e ISO/IEC 27001

8. ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

La Universidad de Cundinamarca establecerá una estrategia de seguridad y privacidad de la información en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que esta estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI.

Por tal motivo, la universidad define las siguientes 7 estrategias específicas, que permitirán establecer en su conjunto una estrategia general

Ilustración 7 Ejes estratégicos de seguridad de la información

8.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del Modelo de Seguridad y Privacidad de la Información – MSPI.

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Universidad de Cundinamarca a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Planificación de la seguridad de la información	Identificar, valorar y clasificar los activos de información más importantes del negocio, para poder así determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la Universidad de Cundinamarca en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Universidad de Cundinamarca, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.
Gestión de Cumplimiento	Identificar y administrar los riesgos de carácter jurídico que puede afrontar la organización, con respecto a incidentes presentados sobre sus activos de información, que se puede generar sobre diferentes componentes.
Evaluación de desempeño de seguridad y privacidad de la información	Evaluar el desempeño y la eficacia del Sistema de Gestión de Seguridad de la Información – SGSI.

Tabla 3. Estrategias específicas para la implementación del SGSI
Fuente: Plan Estratégico de Seguridad de la Información (PESI)
Adaptada para la Universidad del Cundinamarca

8.2 ALINEACIÓN DE LOS EJES ESTRATÉGICOS DE SEGURIDAD DEL PESI CON LA ISO/IEC 27002:2022 Y EL PETI

Los ejes estratégicos definidos en el PESI permiten estructurar y priorizar las acciones institucionales en materia de seguridad y privacidad de la información. A continuación, se presenta una matriz que evidencia cómo cada eje se alinea con los controles establecidos en la norma ISO/IEC 27002:2022 y con los Objetivos Estratégicos de TI (OETI) definidos en el PETI, asegurando así una integración transversal entre el marco normativo internacional, los requerimientos institucionales y los proyectos tecnológicos de la Universidad de Cundinamarca. Esta alineación refuerza la gobernanza, la resiliencia operativa, y el cumplimiento normativo en el contexto de transformación digital.

Eje Estratégico de Seguridad	Propósito	Controles ISO/IEC 27002:2022	Resultados Esperados	OETI Relacionado (PETI)
1. Liderazgo de seguridad de la información	Establece el marco de gobernanza institucional para la seguridad. Define políticas, roles y responsabilidades, fortaleciendo el compromiso directivo.	A.5.1, A.5.2, A.5.4, A.5.5	- Política general de seguridad de la información - Resolución de adopción del SGSI - Manual ESG-SSI-M004 de roles y responsabilidades - Comité de Seguridad formalizado	**OETI2**, **OETI4**
2. Planificación de la seguridad de la información	Permite identificar y gestionar riesgos a través del inventario de activos, evaluación de riesgos y diseño del plan de tratamiento. Establece las bases del SGSI.	A.5.3, A.5.12, A.8.1, A.5.32	- Matriz de activos y clasificación - Mapa de riesgos institucionales - Plan de tratamiento de riesgos - Declaración de aplicabilidad (SoA)	**OETI2**, **OETI4**
3. Concientización	Impulsa la cultura organizacional de seguridad mediante formación, comunicación interna y participación activa	A.6.3, A.6.4, A.5.5	- Programa de concientización anual - Materiales de capacitación - Registros de asistencia y evaluaciones	**OETI2**, **OETI3**

Eje Estratégico de Seguridad	Propósito	Controles ISO/IEC 27002:2022	Resultados Esperados	OETI Relacionado (PETI)
	del personal en el SGSI.		- Encuestas de percepción de cultura de seguridad	
4. Implementación de controles	Ejecuta medidas tecnológicas y administrativas que materializan los objetivos de seguridad definidos. Se enfoca en la protección práctica de los activos.	A.8.x (todos los controles técnicos), A.5.18, A.8.15, A.8.16	- Plan operacional del SGSI - Registros de implementación de controles - Reportes técnicos (firewalls, antivirus, DLP, etc.) - Manuales e instructivos de operación segura	**OETI2**, **OETI4**, **OETI5**
5. Gestión de incidentes	Establece protocolos de detección, análisis, reporte, respuesta y recuperación ante eventos de seguridad. Disminuye el impacto y asegura trazabilidad.	A.5.24, A.5.25, A.5.26, A.5.27	- Procedimiento de gestión de incidentes - Formatos de notificación y respuesta - Bitácoras de incidentes y evidencias - Reportes a la Alta Dirección	**OETI2**, **OETI4**
6. Gestión de cumplimiento	Permite identificar obligaciones legales, normativas y contractuales. Administra los riesgos jurídicos asociados al tratamiento de datos y uso de tecnologías.	A.5.31, A.5.33, A.5.34, A.5.35	- Registro de requisitos legales aplicables - Auditorías de cumplimiento - Reportes de cumplimiento normativo - Procedimientos de revisión legal periódica	**OETI1**, **OETI2**, **OETI3**

Eje Estratégico de Seguridad	Propósito	Controles ISO/IEC 27002:2022	Resultados Esperados	OETI Relacionado (PETI)
7. Evaluación de desempeño de seguridad y privacidad de la información	Este eje garantiza la mejora continua del SGSI mediante el monitoreo sistemático, auditorías internas y revisiones por la dirección. Evalúa la eficacia de los controles implementados y la adherencia al PESI y al marco legal. Proporciona insumos clave para la toma de decisiones, priorización de recursos y reajuste de estrategias.	A.5.35 A.5.5 Cláusula 9 y 10	- Plan de auditoría interna SGSI - Informes de auditoría con hallazgos y acciones - Informe de revisión por la dirección - Indicadores de desempeño - Planes de mejora derivados de resultados	**OETI2**, **OETI4**, **OETI1**

Tabla 4 Alineación de los Ejes Estratégicos de Seguridad del PESI con la ISO/IEC 27002:2022 y el PETI

8.3 PORTAFOLIO DE PROYECTOS / ACTIVIDADES

Para cada estrategia específica, la Universidad de Cundinamarca define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información - SGSI:

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad y privacidad de la información	**Proyecto 1:** Garantizar el liderazgo y el compromiso de la alta dirección **Proyecto 2:** Determinar los elementos externos e internos que son relevantes para la seguridad y privacidad de la información **Proyecto 3:** Determinar partes interesadas internas o externas que pueden influir directamente en la seguridad y privacidad de	Acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces Análisis DOFA del SGSI Matriz de Partes Interesadas Política de Seguridad Formalizada e

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	la información **Proyecto 4:** Desarrollar e implementar una política de seguridad **Proyecto 5:** Definición de Roles y Responsabilidades de Seguridad de la Información.	Implementada. Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
Planificación de la seguridad y privacidad de la información	**Proyecto 1:** Estructurar una metodología que permita identificar y clasificar los activos de información **Proyecto 2:** Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información. **Proyecto 3:** Definir planes de tratamiento de riesgos de seguridad **Proyecto 4:** Determinar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.	Procedimiento de inventario y clasificación de la información Procedimiento y metodología de gestión de riesgos de seguridad de la información institucional Plan de tratamiento de riesgos Banco de proyectos Institucional Matriz de medición del SGSI
Concientización	**Proyecto 1:** Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información **Proyecto 2:** Realizar jornadas de sensibilización a todo el personal.	Plan de Sensibilización Matriz de Flujos de comunicaciones Evidencias de las actividades desarrolladas
Implementación de controles	**Proyecto 1:** Implementar los planes y controles para lograr los objetivos del SGSI	Plan de implementación de controles de seguridad y

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
		privacidad de la información Declaración de Aplicabilidad Herramienta de diagnóstico de seguridad y privacidad de la información
Gestión de incidentes	**Proyecto 1:** Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. **Proyecto 2:** Gestionar los eventos y/o incidentes de seguridad y privacidad de la información.	Procedimiento de gestión de incidentes de seguridad formalizado. Reporte y Consolidado de eventos y/o incidentes de seguridad y privacidad de la información
Gestión de cumplimiento	**Proyecto 1:** Implementación del Programa Integral de Gestión de Datos Personales	Reporte de las RNBD de la SIC Política de Tratamiento de Datos Personales actualizada
Evaluación de desempeño de seguridad y privacidad de la información	**Proyecto 1:** Definir los indicadores de seguridad y privacidad de la información, para evaluar el desempeño y la eficacia del SGSI. **Proyecto 3:** Realizar las auditorías internas con el fin de obtener información sobre el cumplimiento del SGSI **Proyecto 4:** Presentar el avance de la implementación del SGSI a la alta dirección	Matriz de medición de seguridad y privacidad de la información Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información Resultados de las auditorías internas. Acta y documento de Revisión por la Dirección. Compromisos de la Revisión por la Dirección.

Tabla 5: Proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continua del SGSI
Fuente: Plan Estratégico de Seguridad de la Información (PESI)
Adaptada para la Universidad del Cundinamarca

8.4 ALINEACIÓN ENTRE PROYECTOS DEL PESI Y DEL PETI

En el marco de la integración institucional entre la seguridad de la información y las tecnologías de la información, la siguiente tabla presenta la alineación entre los proyectos definidos en el PESI y los proyectos estratégicos del PETI de la Universidad de Cundinamarca. Esta articulación garantiza que las iniciativas tecnológicas estén respaldadas por medidas de seguridad, cumplimiento normativo y gestión de riesgos, permitiendo una transformación digital segura, sostenible y conforme al Sistema de Gestión de Seguridad de la Información (SGSI) y la norma ISO/IEC 27001:2022.

OETI (PETI)	Proyecto PETI	Proyectos del PESI Alineados	Productos / Resultados Esperados
OETI1: Fortalecer la Gobernanza de Datos	- Proyecto Unificado de Arquitectura Empresarial - Taller de Uso y Apropiación	- Proyecto 1, 2 y 3 del eje Liderazgo - Proyecto 1 y 2 del eje Planificación - Proyecto del eje Gestión de Cumplimiento	- Política de seguridad - Matriz de partes interesadas - DOFA - Roles y responsabilidades - Registro RNBD - Política de tratamiento de datos actualizada
OETI2: Reforzar la Seguridad Integral	- Seguridad Informática - Oficial de Protección de Datos	- Proyectos de los ejes: Implementación de controles, Gestión de Incidentes, Gestión de Cumplimiento, Evaluación de Desempeño	- Declaración de aplicabilidad - Procedimiento de incidentes - Reportes de eventos - Indicadores del SGSI - Auditorías y revisión por la dirección
OETI3: Continuar la Transformación Digital	- Bus de Integración - Fábrica de Software - Migración a Nube - Renovación de Plataforma	- Proyecto 4 del eje Planificación - Proyecto 1 del eje Implementación de controles - Proyecto 2 del eje Concientización	- Plan de implementación de controles - Herramienta de diagnóstico - Sensibilización y flujos de comunicación

	- Fortalecimiento de Infraestructura		
OETI4: Optimizar la operación de TI	- Licencias de software - Control de acceso - Servidores físicos y virtuales - Contratación de personal	- Proyecto 3 del eje Planificación - Proyecto 1 del eje Implementación de controles - Proyectos del eje Evaluación de Desempeño	- Plan de tratamiento de riesgos - Declaración de aplicabilidad - Matriz de medición - Auditorías internas SGSI
OETI5: Adoptar Tecnologías Innovadoras	- Wifi CAD - Diplomas - Blockchain.	- Proyectos de los ejes: Planificación, Implementación, Evaluación	- Diagnóstico de seguridad para tecnologías emergentes - Controles específicos definidos - Evidencia de auditoría de entornos disruptivos

9. CRONOGRAMA DEL PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La coordinadora del Sistema de Gestión de Seguridad de la Información – SGSI, con base a los proyectos definidos en la sección anterior, estableció un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos, este se socializa cada vigencia en la primera comisión de gestión ordinaria o extraordinaria, para su aprobación y posterior aprobación por parte de la alta dirección.

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.

Es importante aclarar que dependiendo de la madurez del SGSI en la Universidad de Cundinamarca 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 y la documentación respectiva dispuesta por el MinTIC, en materia de Seguridad de la Información, para las entidades del gobierno colombiano.

10. ESTRATEGIA DE COMUNICACIÓN DEL PESI

Con el fin de asegurar la apropiación del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) en todos los niveles de la Universidad de Cundinamarca, su difusión y

seguimiento se realizarán de forma coordinada a través del ESG-SSI-PL01 - Plan Institucional de Sensibilización y Entrenamiento en Seguridad y Privacidad de la Información. Este plan, ya establecido por la institución, contempla los canales, partes interesadas, frecuencias y responsabilidades necesarias para garantizar una comunicación efectiva y continua en materia de seguridad y privacidad.

A través de esta articulación, se busca posicionar al PESI como un eje transversal del PETI y de la transformación digital segura, difundir las responsabilidades individuales y colectivas definidas en el SGSI, comunicar oportunamente riesgos, alertas e incidentes que afecten la seguridad de la información, y promover la apropiación cultural de la seguridad y la privacidad como principios institucionales.

11. ANÁLISIS PRESUPUESTAL

Teniendo en cuenta los proyectos definidos para la implementación de las estrategias contempladas en Seguridad y Privacidad de la Información, se inscribió en el Banco Universitario de Programas y Proyectos, el proyecto denominado "***Implementación del Sistema de Gestión de Seguridad de la Información y la Ley de Protección de Datos Personales",*** en la vigencia 2026, con una asignación presupuestal de $733.516.594

Nota: *El análisis de presupuestal por dinámica institucional es presentado y aprobado a la alta dirección de la Universidad de Cundinamarca, en la vigencia actual para ser ejecutado en la siguiente vigencia.*

AÑO 2026	
PROYECTO	**INVERSIÓN**
Contratación mediante la modalidad de Término Fijo para la vigencia 2026, con los siguientes cargos: (3) Profesional I (1) Profesional (4) Técnico II (2) Técnico	$281.637.648
Contratar la adquisición de un software de análisis de vulnerabilidades para la identificación, gestión y mitigación de riesgos de seguridad y privacidad de la información para la Universidad de Cundinamarca en la sede Fusagasugá, seccionales Girardot y Ubaté, extensiones Chía, Zipaquirá, Soacha y Facatativá, y la oficina de Bogotá	$143.060.500
Contratación del Servicios de Análisis de Impacto del Negocio (BIA) Plan de Recuperación de Desastres (DRP) alcance tecnológico.	$ 210,688,888.21

AÑO 2026	
PROYECTO	**INVERSIÓN**
Adquirir el servicio de apoyo logístico para llevar a cabo las actividades del Sistema de Gestión de Seguridad de la Información – SGSI en la sede Fusagasugá, seccionales Girardot y Ubaté, extensiones Chía, Zipaquirá, Soacha y Facatativá, y la oficina de Bogotá de la vigencia 2026.	$ 12.941.475
Auditoría de Certificación del Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad de Cundinamarca bajo la Norma ISO NTC 27001:2022 en la vigencia 2026	$ 66.746.302
Adquirir el servicio de Auditoría Interna IV del Sistema de Gestión de Seguridad de la Información – SGSI bajo la norma ISO27001:2022.	$83.016.476
Prestar servicios profesionales para la implementación de la Ley de Protección de Datos Personales en la Universidad de Cundinamarca, de acuerdo con la normatividad legal vigente.	$48.580.582
Prestar servicios profesionales para asesorar la transición del Sistema de Gestión de Seguridad de la Información – SGSI, de la norma ISO 27001:2013 a la norma ISO 27001:2022, en la Universidad de Cundinamarca.	$48.580.582
Prestar servicios profesionales para realizar los documentos requeridos para generar la Política de Seguridad Digital y Ciberseguridad del Sistema de Gestión de Seguridad de la Información - SGSI.	$48.953.029
Total, presupuesto año 2026	**$733.516.594**

Tabla 4: Análisis presupuestal para la implementación y mejoramiento continua del SGSI 2026
Fuente: Plan Estratégico de Seguridad de la Información (PESI)
Adaptada para la Universidad del Cundinamarca

12. BIBLIOGRAFÍA Y WEBGRAFÍA

MinTIC. (s.f.). El Modelo de Seguridad y Privacidad de la Información (MSPI). Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

Plan de seguridad y privacidad de la información - Plan de seguridad y privacidad de la información. (s/f). MINTIC Colombia. Recuperado el 23 de enero de 2025, de https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-laCiudadania/Transparencia/135830:Plan-de-seguridad-y-privacidad-de-la-informacion

Manual de Gobierno Digital - Seguridad y privacidad de la información. (s/f). Gov.co. Recuperado el 23 de enero de 2025, de https://gobiernodigital.mintic.gov.co/692/w3-multipropertyvalues-533221-533236.html?_noredirect=1

Plan Estratégico de Tecnologías de la Información y las. (s. f.). Minciencias.https://www.minciencias.gov.co/sites/default/files/upload/planeacion/plan_estrategico_de_tecnologias_de_la_informacion_peti_y_transformacion_digital_2025.pdf

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2025	02	24	Emisión del documento.
2	2025	12	05	Modificaciones de acuerdo con lo dispuesto en la ISO/IEC 27001:2022 y se incluye una sección relacionada con la alineación del PESI con el PETI.
3	2026	01	29	Se actualizó el numeral 6, correspondiente a la referencia del Modelo de Seguridad y Privacidad de la Información (MSPI), incorporando la Resolución 144 de 2025, "Por la cual se designa al Coordinador del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de la Universidad de Cundinamarca". Así mismo, en el numeral 5 Normativa, se actualizó la ubicación del documento AJUr011 "Matriz de identificación y seguimiento al cumplimiento de requisitos legales y otros". En la Fase 7 Metodología e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), se actualizaron las Ilustraciones 2, 3 y 4, correspondientes al Análisis GAP del SGSI, así como la Tabla 1: Resultados de la evaluación del Anexo A de la Norma ISO/IEC 27001:2013 frente al MSPI. Adicionalmente, se realizó la actualización de la Fase 11 Análisis presupuestal, específicamente la Tabla 4: "Análisis presupuestal para la implementación y el mejoramiento continuo del SGSI – vigencia 2026".

ELABORÓ	
NOMBRES Y APELLIDOS	CARGO
Valery Cruz Rodríguez	Técnico II
Brayan Alexis Galindo Ramírez	Profesional

REVISÓ	
NOMBRES Y APELLIDOS	CARGO
María del Pilar Delgado Rodríguez	Coordinadora del Sistema de Gestión de Seguridad de la Información

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del Sistema de Gestión de Seguridad de la Información	2026	01	29