

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 1 de 28

UNIVERSIDAD DE CUNDINAMARCA

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**FUSAGASUGÁ
2025**

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 2 de 28

TABLA DE CONTENIDO

1.	INTRODUCCIÓN.....	3
2.	OBJETIVOS:.....	4
2.1	Objetivo general.....	4
2.2	Objetivo específicos.....	4
3.	ALCANCE:	5
4.	DEFINICIONES.....	6
5.	NORMATIVIDAD.....	7
6.	LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	8
7.	ROLES Y RESPONSABILIDADES EN seguridad y privacidad de la información	9
8.	METODOLOGÍA E IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI.....	10
8.1	CICLO DE OPERACIÓN.....	10
8.2	FASES DEL CICLO OPERATIVO.....	11
8.3	FASE 2. PLANIFICACIÓN (EN EL CICLO PHVA: PLANEAR).....	14
8.4	FASE 3. OPERACIÓN (EN EL CICLO PHVA: HACER).....	15
8.5	FASE 4. EVALUACIÓN DE DESEMPEÑO (EN EL CICLO PHVA: VERIFICAR).....	16
8.6	FASE 5. MEJORAMIENTO CONTINUO (EN EL CICLO PHVA: ACTUAR) 16	
8.7	ALINEACIÓN NORMA ISO 27001:2013 VS CICLO DE OPERACIÓN.....	17
9.	CRONOGRAMA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	18
9.1	DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES).....	18
9.2	PORTAFOLIO DE PROYECTOS / ACTIVIDADES.....	20
10.	ANÁLISIS PRESUPUESTAL.....	25
11.	BIBLIOGRAFÍA Y WEBGRAFÍA.....	27

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 3 de 28

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI), desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), constituye una guía fundamental para fortalecer la protección de la información en las organizaciones, integrando las mejores prácticas de la norma ISO/IEC 27001:2022 y cumpliendo con las disposiciones normativas vigentes en Colombia relacionadas con la seguridad y privacidad de la información.

En este contexto, la Universidad de Cundinamarca ha diseñado el presente Plan de Seguridad y Privacidad de la Información, con el objetivo de priorizar la implementación de la norma y los controles requeridos, garantizando un enfoque sistemático basado en el ciclo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar). Este plan refleja el compromiso institucional con la adopción de un Sistema de Gestión de Seguridad de la Información robusto y un Programa Integral de Gestión de Datos Personales, orientados a proteger la confidencialidad, integridad y disponibilidad de la información en todos los niveles de la universidad.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 4 de 28

2. OBJETIVOS:

2.1 OBJETIVO GENERAL

Establecer un Plan Estratégico de Seguridad y Privacidad de la Información para fortalecer la confidencialidad, integridad, disponibilidad de los activos de la información de la Universidad de Cundinamarca, a partir de la implementación de las estrategias de seguridad, privacidad y ciberseguridad de la información.

2.2 OBJETIVO ESPECÍFICOS

- Definir las etapas para establecer la estrategia de seguridad y privacidad de la información en la Universidad de Cundinamarca.
- Definir y establecer las necesidades de la institución para la implementación del Sistema de Gestión de Seguridad de la Información - SGSI.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.
- 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 y privacidad de la información.
- Establecer la línea base para que la Universidad de Cundinamarca 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.
- Promover la mejora continua, involucrando a todas las partes interesadas en los procesos de implementación del SGSI.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 5 de 28

3. ALCANCE:

El presente documento establece el grado de avance en la implementación de las actividades necesarias para lograr de manera progresiva y efectiva el Plan Estratégico de Seguridad y Privacidad de la Información, el cual se realizara por medio de cronogramas de actividades por vigencia, para el Sistema de Gestión de Seguridad de la Información – SGSI y la Ley de Protección de Datos Personales, socializado en la Comisión de Gestión, Atendiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital y conforme a la disponibilidad de los recursos asignados por banco de Proyectos de la Universidad de Cundinamarca.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 6 de 28

4. DEFINICIONES

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:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable, cuando lo requiera una entidad autorizada.
- **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.
- **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. (ISO/IEC 27000).
- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 7 de 28

5. NORMATIVIDAD

La normatividad externa como son Constitución, leyes, decretos, resoluciones y demás, se encuentra documentada 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 del Sistema de Gestión de Seguridad de la Información y el Programa Integral de Gestión de Datos Personales, se encuentra publicada, en el Modelo de Operación Digital, en el proceso Sistemas Integrados, Seguridad de la Información, en el link <https://www.ucundinamarca.edu.co/sgc/index.php/macroproceso-estrategico/proceso-gestion-sistemas-integrados/sgsi>

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 8 de 28

6. LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Universidad de Cundinamarca, atendiendo la normatividad y lineamientos establecidos en el *DOCUMENTO MAESTRO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN* - Ministerio de Tecnologías de la Información y las Comunicaciones OCTUBRE 2021.

De conformidad con **Roles y responsabilidades**, la institución mediante Resolución 140 de 2022 “*POR LA CUAL SE DESIGNA EL COORDINADOR DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI Y LA PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD DE CUNDINAMARCA*”, con el fin de poder realizar la labor de implementación del SGSI de manera eficiente, la entidad debe designar a un responsable de seguridad de la información, quien será el líder del proyecto, con la competencia, formación, experticia y experiencia apropiada, el cual dependerá de la Alta Dirección y que estará articulado con los demás sistemas de gestión de la entidad.

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”*.

Los lineamientos anteriormente descritos, hacen parte del Manual ESG-SSI-M001 - MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, a nivel institucional.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 9 de 28

7. ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Continuando con el diseño, implementación, operación y mejora continua del SGSI, la Universidad de Cundinamarca, a partir de los directrices y lineamientos establecidos y adoptadas por el Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando el despliegue de las directrices de seguridad en todas las áreas académico administrativas de la institución y monitoreando constantemente su cumplimiento para tomar las acciones necesarias que permitan garantizar la seguridad de la información.

Es así, que se establece 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.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 10 de 28

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

8.1 CICLO DE OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla 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 Diagnóstico: 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.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 11 de 28

- 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.

8.2 FASES DEL CICLO OPERATIVO.

8.2.1 FASE I: DIAGNOSTICO.

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 27001:2013 es del **68%**, como se detalla en el siguiente gráfico.

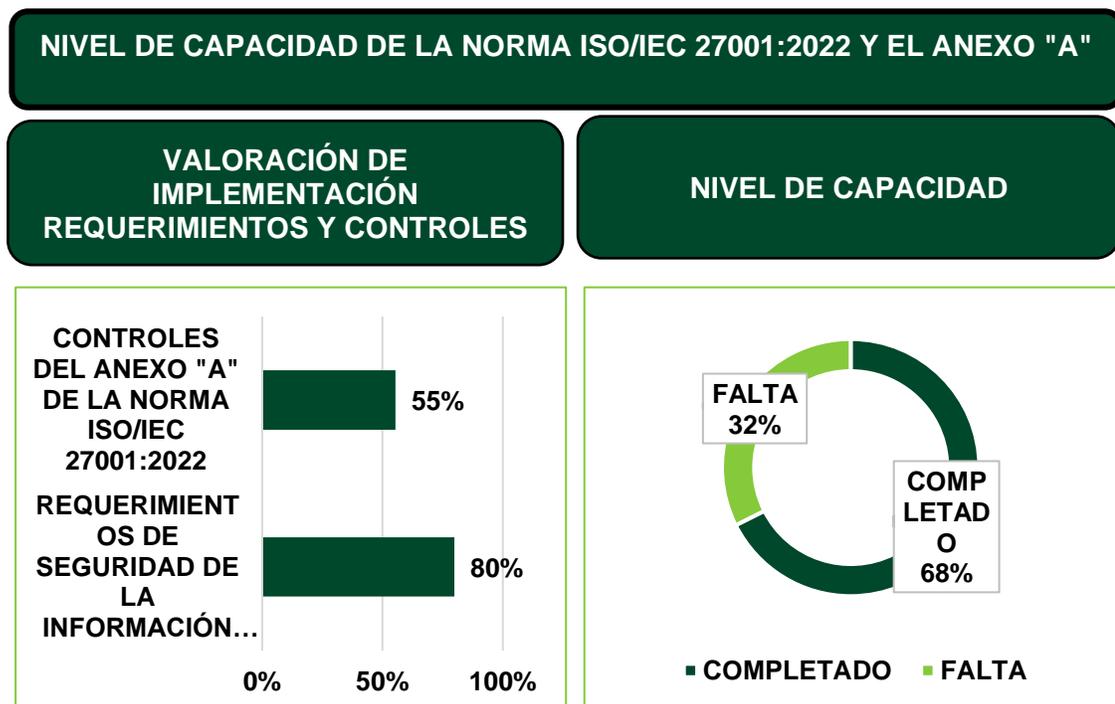
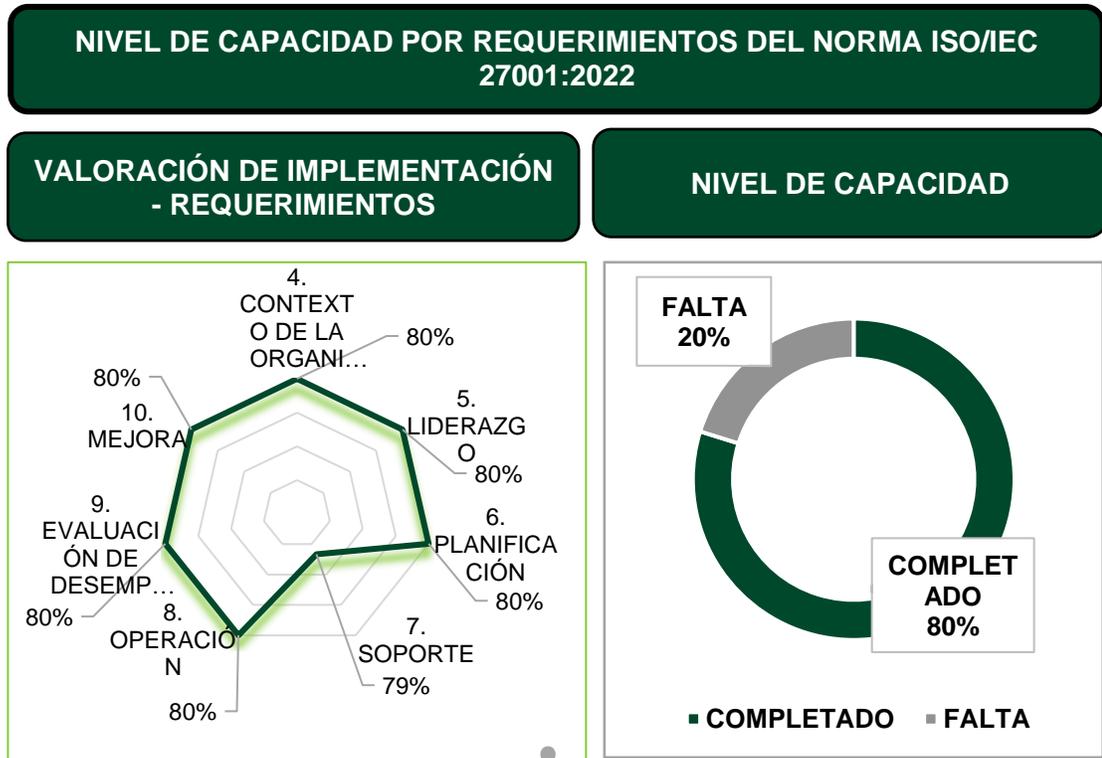


Ilustración 2. Análisis GAP del SGSI
Fuente: Propia - Universidad del Cundinamarca

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 12 de 28

Este avance se distribuye en dos áreas 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 a la implementación de los controles categorizados en Organizacionales, De Personas, Físicos y Tecnológicos, el nivel de avance alcanza es del **55%**, evidenciando áreas de oportunidad que deben ser abordadas para cumplir plenamente con la norma.



	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 13 de 28

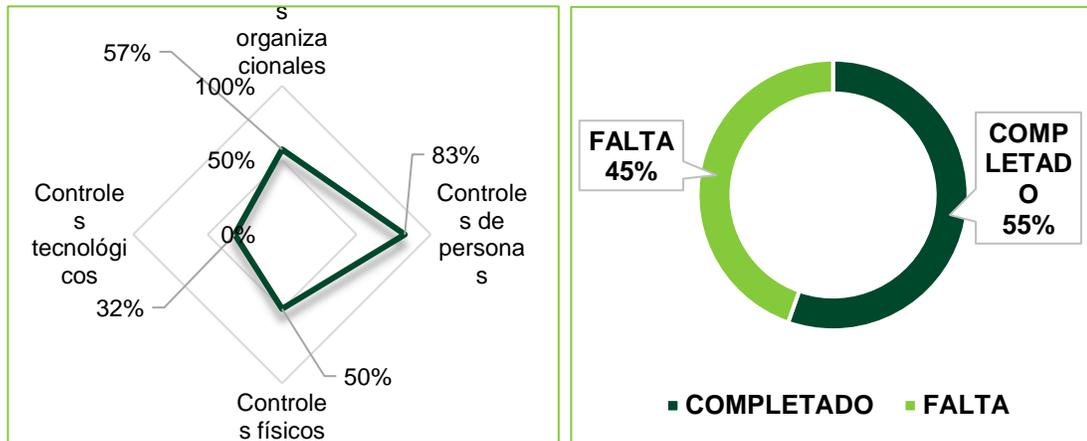


Ilustración 4. Análisis GAP del SGSI
Fuente: Propia - Universidad del Cundinamarca

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 MSPÍ del **68%** encontrado sé en un nivel de madurez “**Efectivo**”, 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*”.

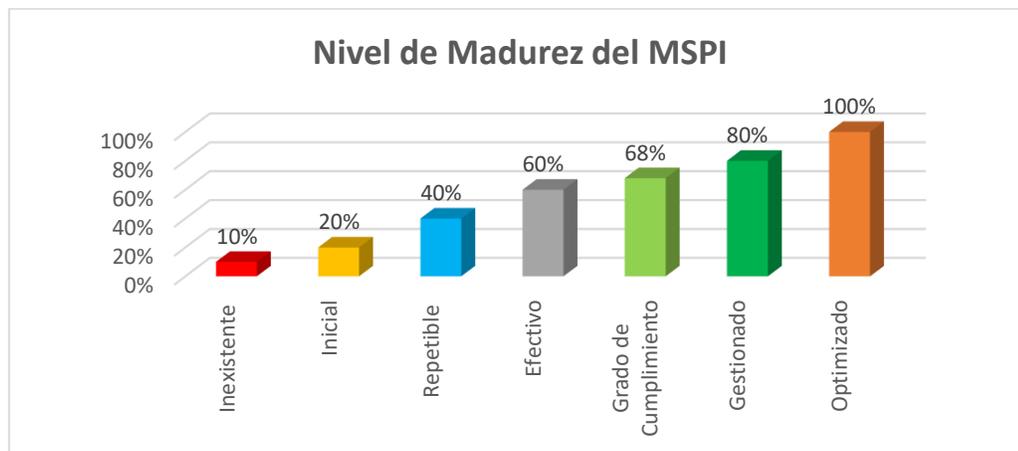


Ilustración 5. Niveles de madurez frente a la implementación del MSPÍ
Fuente: Propia - Universidad del Cundinamarca

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:

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 14 de 28

Evaluación de Efectividad de Control			
Categoría	Calificación Actual	Calificación Objetivo	Evaluación de Efectividad de Control
A.5 Controles Organizacionales	57%	100%	Efectivo
A.6 Controles De Personas	83%	100%	Gestionado
A.7 Controles Físicos	50%	100%	Repetible
A.8 Controles Tecnológicos	32%	100%	Inicial
Promedio evaluación de Controles	55%	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*

8.3 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 SGSI.

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

- a) Contexto: En esta actividad, 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.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 15 de 28

- a) Liderazgo: 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 de Cundinamarca 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 de Seguridad de la Información. Sumado a lo anterior, se tiene presupuesto asignado para fortalecer la seguridad digital e implementar el SGSI.
- b) 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 manera, se realizó el diseño de toda la documentación que compone el SGSI con base en los controles establecidos en el Anexo A de la Norma ISO/IEC 27001:2013 (Procedimientos, manuales, formatos, guías, instructivos).
- c)) 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 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 SGSI en cada vigencia.

8.4 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 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 SGSI. Dentro de las actividades de esta fase se contempla:

- a) Implementar el plan Operacional de Seguridad de la información.
- 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.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 16 de 28

d) Monitoreo y seguimiento a la implementación de controles de seguridad de la información.

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

Una vez se haya terminado la fase de Operación se lleva a cabo la fase de Evaluación de desempeño, la cual permite a la Universidad de Cundinamarca 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 de la Información - SGSI en la institución. Dentro de esta fase se contemplan las siguientes actividades:

- a) Seguimiento, medición, análisis y evaluación. En esta actividad el SGSI garantizará que se conozca de manera permanente la gestión que se ha realizado para la adopción del MSPI, así como sus logros y metas.
- b) Auditoría Interna. La universidad realizará auditorías Internas al Sistema de Gestión de Seguridad de la información SGSI 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 SGSI realizará el reporte respectivo de la información resultante de las evaluaciones de desempeño del MSPI, incidentes, comportamientos y demás aspectos relevantes para que la dirección se encuentre al tanto y le permita determinar su conveniencia, adecuación y eficacia.

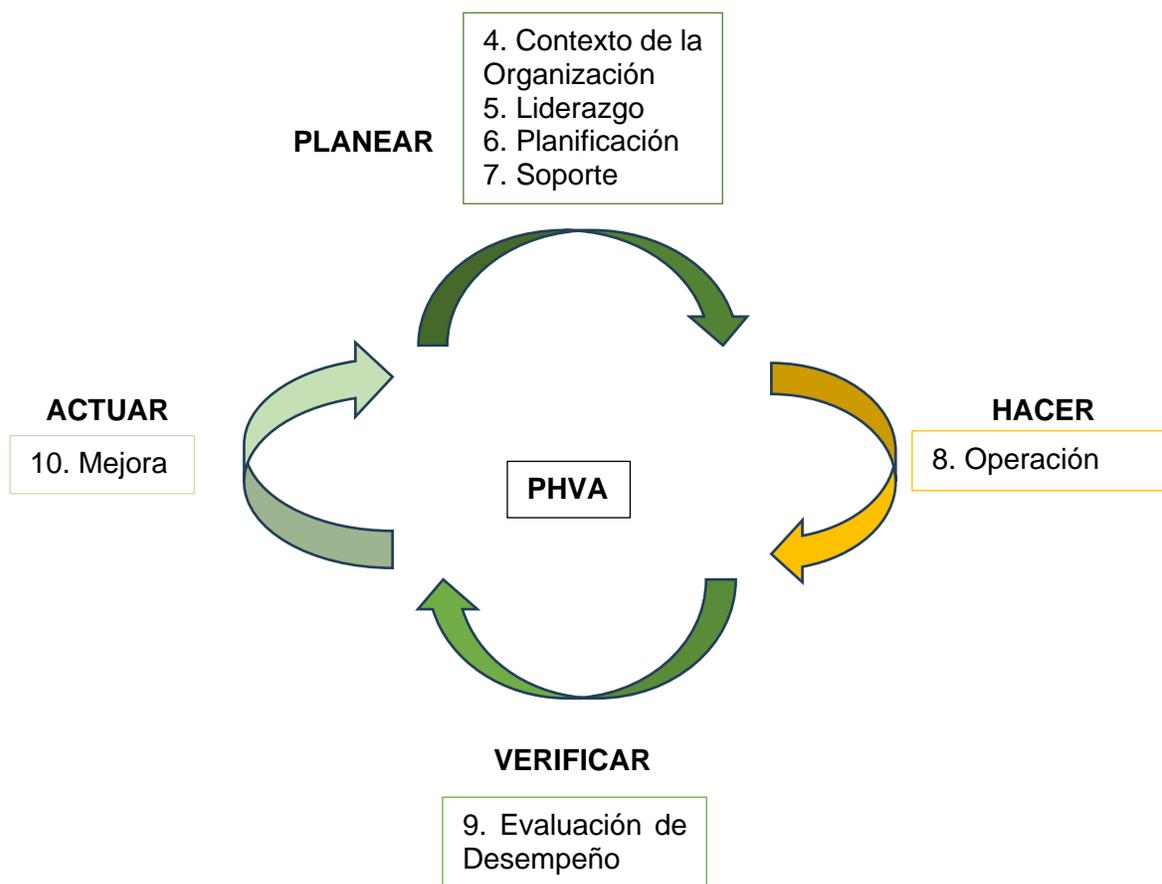
8.6 FASE 5. MEJORAMIENTO CONTINUO (EN EL CICLO PHVA: ACTUAR)

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 SGSI. Como resultado de esta fase se debe actualizar el “Plan de Seguridad y Privacidad de la Información” así como el 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 institución.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 17 de 28

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

Aunque en la norma ISO 27001:2022 no se 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 las modelos de gestión de la siguiente forma:



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

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 18 de 28

9. CRONOGRAMA DEL PLAN 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.

9.1 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.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 19 de 28

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
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

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 20 de 28

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
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 2. Estrategias específicas para la implementación del SGSI
Fuente: [Plan Estratégico de Seguridad de la Información \(PESI\)](#)
Adaptada para la Universidad de Cundinamarca

9.2 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	<p>Proyecto 1: Garantizar el liderazgo y el compromiso de la alta dirección</p> <p>Proyecto 2: Determinar los elementos externos e internos que son relevantes para la seguridad y privacidad de la información</p> <p>Proyecto 3: Determinar partes interesadas internas o externas que pueden influir directamente en la seguridad y privacidad de la información</p> <p>Proyecto 4: Desarrollar e implementar una política de seguridad</p>	<p>Acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces</p> <p>Análisis DOFA del SGSI</p> <p>Matriz de Partes Interesadas</p> <p>Política de Seguridad Formalizada e Implementada.</p> <p>Definición de los Roles y Responsabilidades</p>

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 21 de 28

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	<p>Proyecto 5: Definición de Roles y Responsabilidades de Seguridad de la Información.</p>	<p>en Seguridad de la Información formalizados dentro de las políticas de seguridad.</p>
<p>Planificación de la seguridad y privacidad de la información</p>	<p>Proyecto 1: Estructurar una metodología que permita identificar y clasificar los activos de información</p> <p>Proyecto 2: Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información.</p> <p>Proyecto 3: Definir planes de tratamiento de riesgos de seguridad</p> <p>Proyecto 4: Determinar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.</p>	<p>Procedimiento de inventario y clasificación de la información y</p> <p>Procedimiento y metodología de gestión de riesgos de seguridad de la información institucional</p> <p>Plan de tratamiento de riesgos</p> <p>Banco de proyectos Institucional</p> <p>Matriz de medición del SGSI</p>

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 22 de 28

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Concientización	<p>Proyecto 1: Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información</p> <p>Proyecto 2: Realizar jornadas de sensibilización a todo el personal.</p>	<p>Plan de Sensibilización</p> <p>Matriz de Flujos de comunicaciones</p> <p>Evidencias de las actividades desarrolladas</p>
Implementación de controles	<p>Proyecto 1: Implementar los planes y controles para lograr los objetivos del SGSI</p>	<p>Plan de implementación de controles de seguridad y privacidad de la información</p> <p>Declaración de Aplicabilidad</p> <p>Herramienta de diagnóstico de seguridad y privacidad de la información</p>

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 23 de 28

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Gestión de incidentes	<p>Proyecto 1: Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.</p> <p>Proyecto 2: Gestionar los eventos y/o incidentes de seguridad y privacidad de la información.</p>	<p>Procedimiento de gestión de incidentes de seguridad formalizado.</p> <p>Reporte y Consolidado de eventos y/o incidentes de seguridad y privacidad de la información</p>
Gestión de cumplimiento	<p>Proyecto 1: Implementación del Programa Integral de Gestión de Datos Personales</p>	<p>Reporte de las RNBD de la SIC</p> <p>Política de Tratamiento de Datos Personales actualizada</p>

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 24 de 28

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Evaluación de desempeño de seguridad y privacidad de la información	<p>Proyecto 1: Definir los indicadores de seguridad y privacidad de la información, para evaluar el desempeño y la eficacia del SGSI.</p> <p>Proyecto 3: Realizar las auditorías internas con el fin de obtener información sobre el cumplimiento del SGSI</p> <p>Proyecto 4: Presentar el avance de la implementación del SGSI a la alta dirección</p>	<p>Matriz de medición de seguridad y privacidad de la información</p> <p>Plan de auditorías que evidencia la programación de las auditorías de seguridad y privacidad de la información</p> <p>Resultados de las auditorías internas.</p> <p>Acta y documento de Revisión por la Dirección.</p> <p>Compromisos de la Revisión por la Dirección.</p>

Tabla 3: 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

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 25 de 28

10. 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 2025, con una asignación presupuestal de \$ 575,558,033.

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 2025	
PROYECTO	INVERSIÓN
Contratación del servicio del rol de Oficial de Protección de Datos Personales en cumplimiento y acorde al Programa Integral de Gestión de Datos Personales – PIGDP de la Universidad de Cundinamarca de acuerdo con la normatividad legal vigente.	\$ 278,012,147.21
Contratación del Software para el análisis Automático de varias fuentes de información, con el fin de mitigar los riesgos y amenazas virtuales que puedan afectar a la institución y su imagen a nivel corporativo.	\$ 137,847,116.00
Contratación del Servicios de Análisis de Impacto del Negocio (BIA) Plan de Recuperación de Desastres (DRP) alcance tecnológico.	\$ 210,688,888.21
Adquirir el servicio de apoyo logístico para las Jornadas de Sensibilización en Seguridad y Privacidad de la Información en sede, seccionales y extensiones, incluido el Centro Académico Deportivo – CAD y Oficina de Bogotá.	\$ 12,384,187.00

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24
		PAGINA: 26 de 28

Adquirir el servicio de Auditoría Interna III del Sistema de Gestión de Seguridad de la Información – SGSI bajo la norma ISO27001:2022.	\$ 83,081,999.62
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.	\$ 47,206,819.81
Prestar servicios profesionales para orientar la transición del Sistema de Gestión de Seguridad la Información - SGSI, de la norma ISO 27001:2013 a la norma ISO 27001:2022, en la Universidad de Cundinamarca.	\$ 47,206,819.81
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.	\$ 47,206,819.81
Contratación mediante la modalidad de Término Fijo IPA – IIPA 2025 con los siguientes cargos: (3) Profesional I, (3) Técnico III, (2) Técnicos.	\$ 260,477,566.00
Total presupuesto año 2025	\$ 1.124.112.360

Tabla 4: Análisis presupuestal para la implementación y mejoramiento continua del SGSI 2025

Fuente: [Plan Estratégico de Seguridad de la Información \(PESI\)](#)

Adaptada para la Universidad del Cundinamarca

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 27 de 28

11. BIBLIOGRAFÍA Y WEBGRAFÍA

MinTIC. (s.f.). El Modelo de Seguridad y Privacidad de la Información (MSPI).
Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-162623_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-la-Ciudadania/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

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-PL03
	PROCESO GESTIÓN SISTEMAS INTEGRADOS - SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 1
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VIGENCIA: 2025-02-24 PAGINA: 28 de 28

CONTROL DE CAMBIOS						
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO		
	AAAA	MM	DD			
1	2025	02	24	Emisión del documento.		
ELABORÓ						
NOMBRES Y APELLIDOS			CARGO			
Fabian Libardo Parra Gutiérrez			Profesional I			
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		2025	02	24