Universidad del Cauca

DOCUMENTO MAESTRO - SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2025

Transformando la Universidad del Cauca a través de las Tecnologías de la Información

Este documento maestro describe la estructura del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad, en conformidad con los lineamientos y recomendaciones establecidos en la última versión del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC), así como con los requisitos de la norma internacional ISO/IEC 27001:2022.

Versión 0.2 - Abril de 2024

www.unicauca.edu.co

0. Tabla de contenido

1. Introducción

En la actualidad, la Seguridad y Privacidad de la Información se han convertido en pilares fundamentales para el funcionamiento óptimo y responsable de las instituciones educativas. En este contexto, la Universidad del Cauca emprende las acciones necesarias para implementar el Sistema de Gestión de Seguridad de la Información (SGSI), tomando como referencia el Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), una iniciativa estratégica que busca garantizar la protección eficaz de los datos e información de la comunidad universitaria en un entorno cada vez más digital y conectado.

Este documento representa una guía integral para la operación y seguimiento del SGSI en la Universidad del Cauca, proporcionando un marco de trabajo estructurado y alineado con las normativas nacionales propuestas por el MinTIC y normativas internacionales en materia de seguridad de la información y protección de datos tales como la norma ISO 27001:2022, para asegurar que este sistema aborda los desafíos y riesgos específicos a los que se enfrenta el entorno académico en cuanto a la gestión de la información.

A través de este sistema, la Universidad del Cauca se propone fortalecer su cultura organizacional en temas de seguridad y privacidad, desarrollar competencias clave en su personal, y establecer prácticas y procedimientos robustos que aseguren la confidencialidad, integridad y disponibilidad de la información.

Esto incluye no sólo la protección de datos personales y académicos, sino también la salvaguarda de la investigación, la propiedad intelectual y los recursos informáticos de nuestra comunidad universitaria.

El SGSI se presenta como un esfuerzo continuo y evolutivo, comprometido con la mejora y adaptación constantes frente a los cambiantes riesgos de seguridad y privacidad en el ámbito digital. Con este documento, invitamos a toda la comunidad universitaria a participar activamente en la implementación y el fortalecimiento de un entorno digital seguro y confiable para todos.

2. Audiencia

El presente documento del Sistema de Gestión de Seguridad de la Información (SGSI) está dirigido a un amplio espectro de audiencias dentro de la comunidad universitaria, con el objetivo de garantizar una comprensión y participación integral en la Seguridad y Privacidad de la Información. La audiencia incluye, pero no se limita a, los siguientes grupos:

- **Consejo superior, rectoría y vicerrectorías:** Incluye a los miembros del consejo superior, el rector y las vicerrectorías. Este grupo es fundamental para la toma de decisiones estratégicas, la asignación de recursos y el liderazgo en la operación y mantenimiento a largo plazo del SGSI.
- **Personal líder de divisiones y oficinas:** Jefes y líderes de diferentes áreas académicas y administrativas, encargados de supervisar la implementación y el cumplimiento de las actividades y políticas propuestas en el SGSI en sus respectivas divisiones y oficinas.
- **Personal administrativo:** Empleados que trabajan en áreas académicas y administrativas. Estos profesionales son responsables de ejecutar y mantener los procesos y sistemas que protegen la información institucional.

- **Personal de la División TIC y Seguridad de la Información:** Especialistas en tecnologías de la información y seguridad, encargados de la implementación técnica, gestión y monitoreo de las medidas de seguridad informática y privacidad de la información.

- **Auditores y revisores externos:** Profesionales externos que realizan las revisiones y auditorías de seguridad para asegurar el cumplimiento de estándares y normatividad pertinentes.

- **Proveedores y contratistas:** Todos los proveedores y contratistas que trabajan con la Universidad y que manejan, acceden o influyen en la información y los sistemas de la Universidad. Es esencial que estos grupos externos comprendan y se adhieran a las políticas y lineamientos del SGSI para garantizar una gestión de la información coherente y segura en toda la cadena de suministro y operaciones externas.

- **Personal docente y de investigación:** Profesores e investigadores que manejan información sensible y confidencial, incluyendo datos de estudiantes, resultados de investigaciones y propiedad intelectual. Su papel es crucial para aplicar las políticas de seguridad y privacidad en sus actividades diarias.

- **Estudiantes:** Todos los estudiantes de pregrado y posgrado, quienes deben estar conscientes de las políticas de seguridad y privacidad para proteger su propia información personal y académica, además de respetar la confidencialidad de los datos institucionales.

- **Otros Interesados:** Incluye colaboradores, socios, proveedores y cualquier otra entidad que interactúe con la información de la Universidad y que deba cumplir con los lineamientos establecidos en el SGSI.

Este documento es de **lectura obligatoria** para todos los miembros de la comunidad universitaria, con el fin de garantizar un entendimiento uniforme y una aplicación efectiva de las políticas y procedimientos de Seguridad y Privacidad de la Información.

3. Definiciones

- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

- **MSPI (Modelo de Seguridad y Privacidad de la Información):** Es un marco estructurado desarrollado por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia para gestionar la Seguridad y Privacidad de la Información en organizaciones. Proporciona directrices para asegurar la protección, integridad y confidencialidad de los datos. A diferencia del SGSI, que es un sistema implementado por organizaciones para gestionar riesgos de seguridad específicos, el MSPI sirve como modelo de referencia nacional, ofreciendo principios y prácticas generales para la Seguridad y Privacidad de la Información.

- **PETI (Plan Estratégico de Tecnologías de la Información):** Estrategia integral que orienta la gestión y uso de las tecnologías de la información en una organización, alineando los recursos tecnológicos con los objetivos y metas institucionales.

- **Privacidad de la Información:** Se refiere a la protección de datos personales y sensibles contra el acceso, uso, divulgación o tratamiento no autorizado, respetando los derechos individuales y la confidencialidad.

- **Seguridad de la Información:** Conjunto de medidas preventivas y reactivas destinadas a proteger la información (independientemente de su medio de almacenamiento) contra acceso, uso,

divulgación, alteración o destrucción no autorizados, garantizando su confidencialidad, integridad y disponibilidad.

- **Seguridad Informática:** Área dedicada a la protección de la infraestructura computacional y la información contenida en sistemas informáticos frente a amenazas y vulnerabilidades, incluyendo el software, hardware y datos.

- **SGSI (Sistema de Gestión de Seguridad de la Información):** Es un conjunto estructurado de políticas, procesos, y sistemas diseñados para gestionar los riesgos de seguridad sobre la información de una organización, asegurando su confidencialidad, integridad, y disponibilidad. Basado en principios de gestión de riesgos, el SGSI ayuda a identificar, evaluar y mitigar los riesgos de seguridad, a la vez que garantiza el cumplimiento de normativas legales y estándares internacionales como la ISO 27001.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. Justificación y objetivos

La creciente digitalización de los procesos académicos y administrativos en el ámbito universitario conlleva una mayor exposición a riesgos relacionados con la Seguridad y Privacidad de la Información. La implementación del SGSI en la Universidad del Cauca permitirá proteger los activos de información valiosos frente a amenazas internas y externas, asegurando la confidencialidad, integridad y disponibilidad de los datos.

Este sistema es esencial para cumplir con las regulaciones legales vigentes, contribuir a la prevención de incidentes de seguridad, y garantizar la confianza de estudiantes, personal y otros interesados en la gestión segura y privada de sus datos.

Objetivo Principal

Desarrollar, implementar, operar y mantener un Sistema de Seguridad de la Información (SGSI) integral y robusto, que asegure la protección efectiva de la información y los activos digitales de la Universidad, alineado con las mejores prácticas internacionales y la normativa nacional vigente.

Objetivos Específicos

1. Definir y comunicar políticas y procedimientos claros para la gestión de la Seguridad y Privacidad de la Información, asegurando su comprensión y adhesión por parte de toda la comunidad universitaria.

2. Identificar, analizar y tratar los riesgos de Seguridad y Privacidad de la Información de manera proactiva, minimizando la posibilidad de incidentes y sus potenciales impactos.

3. Fomentar una cultura organizacional que priorice la Seguridad y Privacidad de la Información, mediante programas de capacitación y sensibilización para todos los grupos de interés de la Universidad.

4. Establecer y mantener controles técnicos adecuados para salvaguardar la infraestructura tecnológica y los datos contra accesos no autorizados, alteraciones indebidas o pérdida de información.

5. Realizar evaluaciones periódicas y auditorías internas y externas para medir la efectividad del SGSI y promover su mejora continua.

5. Marco jurídico

1. **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

2. **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.

3. **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.

4. **Decreto 1083 de 2015** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

5. **CONPES 3854 de 2016.** Política Nacional de Seguridad Digital.

6. **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.

7. **Decreto 2106 de 2019,** establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

8. **Ley 1955 de 2019:** Transformación Digital (MinTIC): Establece directrices para la digitalización de servicios públicos y la implementación de tecnologías digitales en entidades gubernamentales en Colombia.

9. **Decreto 1008 de 2018:** Política de Gobierno Digital: Define la política para el uso y aprovechamiento de las TIC, promoviendo eficiencia, transparencia y acceso a servicios digitales en la administración pública.

6. Fase 0: Diagnóstico de línea base (2023)

El diagnóstico de línea base realizado por la Universidad del Cauca (diciembre de 2023) proporciona una visión integral del estado actual en relación con los criterios y requerimientos de Seguridad y Privacidad de la Información establecidos por el MinTIC, los cuales están basados en la norma ISO 27001. Este proceso se llevó a cabo como un paso fundamental antes de iniciar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Con este diagnóstico, se ha logrado identificar no solo el nivel de madurez en la implementación del SGSI, sino también una evaluación inicial de las vulnerabilidades técnicas y administrativas que podrían representar riesgos para la Seguridad y Privacidad de la Información en el contexto de la Universidad. Estos resultados son insumo clave para desarrollar estrategias y acciones concretas destinadas a fortalecer la Seguridad y Privacidad de la Información en la Universidad del Cauca, alineando sus operaciones con las mejores prácticas y estándares internacionales establecidos en la norma ISO 27001.

El flujo de trabajo que se siguió en esta fase está alineado con la metodología para el desarrollo del diagnóstico según los lineamientos establecidos por el MinTIC:

Ilustración - Metodología establecida por MinTIC para el desarrollo del diagnóstico

El diagnóstico se basó en la aplicación del Instrumento de Evaluación del MSPI, una herramienta sólida y reconocida proporcionada por el MinTIC.

Nota: Las instrucciones para aplicar el Instrumento de Evaluación del MSPI han sido establecidas directamente por el MinTIC y la información para su uso se encuentra en detalle en el Portal de Gobierno Digital del MinTIC. (Instructivo para el Diligenciamiento del Instrumento de Evaluación del MSPI).

Este Instrumento permite evaluar los siguientes componentes:

- **Brecha Anexo A ISO 27001:** Este componente muestra el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001, y la guía de controles del Modelo de Seguridad de Privacidad de la Información (MSPI). Para este componente se cuenta con la evaluación de criterios distribuidos en dos secciones así:

- Criterios de Pruebas administrativas: Orientados a los temas de seguridad de la información que no están directamente relacionados con la operación técnica y tecnológica de la universidad, y contemplan entre otras cosas la evaluación, implementación, revisión y mejoras de la Política de Seguridad de la Información, la evaluación de las responsabilidades frente a la seguridad de la información, la revisión y evaluación de los acuerdos de confidencialidad, y la revisión de la documentación y formalización de procedimientos de la universidad. Los criterios evaluados en esta sección incluyen los controles dados en la Norma ISO 2700 de los dominios A5, A6, A7, A8, A17 y A18.

- Criterios de Pruebas técnicas: Orientados a evaluar los controles y requisitos técnicos y tecnológicos asociados los dominios A9, A10, A11, A12, A13, A14 y A16 de la Norma ISO 27001; los cuales se evalúan a partir de la operación, iniciativas y responsabilidades llevadas a cabo por la División TIC.

- **Avance PHVA:** Este componente incluye criterios que permiten evaluar el ciclo de implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, el cual refleja el estado de avance frente a cada una de las etapas del ciclo (Planificación, Implementación, Gestión, Mejora continua).

- **Nivel de madurez:** Este componente indica el nivel de madurez en el que se encuentra la Universidad con respecto al Modelo de Seguridad y Privacidad de la Información – MSPI. Este nivel de madurez se determina a partir de la calificación asignada a los criterios de Pruebas Administrativas, Pruebas Técnicas y PHVA.

  Los niveles de madurez establecidos por el MinTIC son los siguientes:

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades que aún no cuentan con una identificación de activos y gestión de riesgos que les permita determinar el grado de criticidad de la información respecto a la seguridad y privacidad, por lo tanto, los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente de planificación del MSPI
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección procesos, lineamientos y controles de seguridad y privacidad de la información. Todos los controles están debidamente documentados, aprobados, implementados, probados y actualizados
Administrado	En este nivel se encuentran las entidades que cuentan con métricas, indicadores y realizan auditorías de seguridad y privacidad de la información, recolectando información para establecer la efectividad de los controles
Optimizado	En este nivel se encuentran las entidades en donde existe un mejoramiento continuo del MSPI, con retroalimentación cualitativa y cuantitativa del modelo

Ilustración - Niveles de Madurez del Modelo de Seguridad y Privacidad de la Información

Valoración de los criterios

La valoración de los criterios indicados en el Instrumento de Evaluación del MSPI, se realizó con base en la escala de valoración definida por el MinTIC, en la cual se definen los niveles que permiten dar una calificación a cada criterio según la situación que se evidencia al momento de realizar el diagnóstico:

Descripción	Calificación	Condiciones
No aplica	No aplica	No aplica
Inexistente	0	• Total falta de cualquier proceso reconocible. • No se aplican controles.
Inicial	20	• Hay una evidencia de que la Organización ha reconocido que existe un

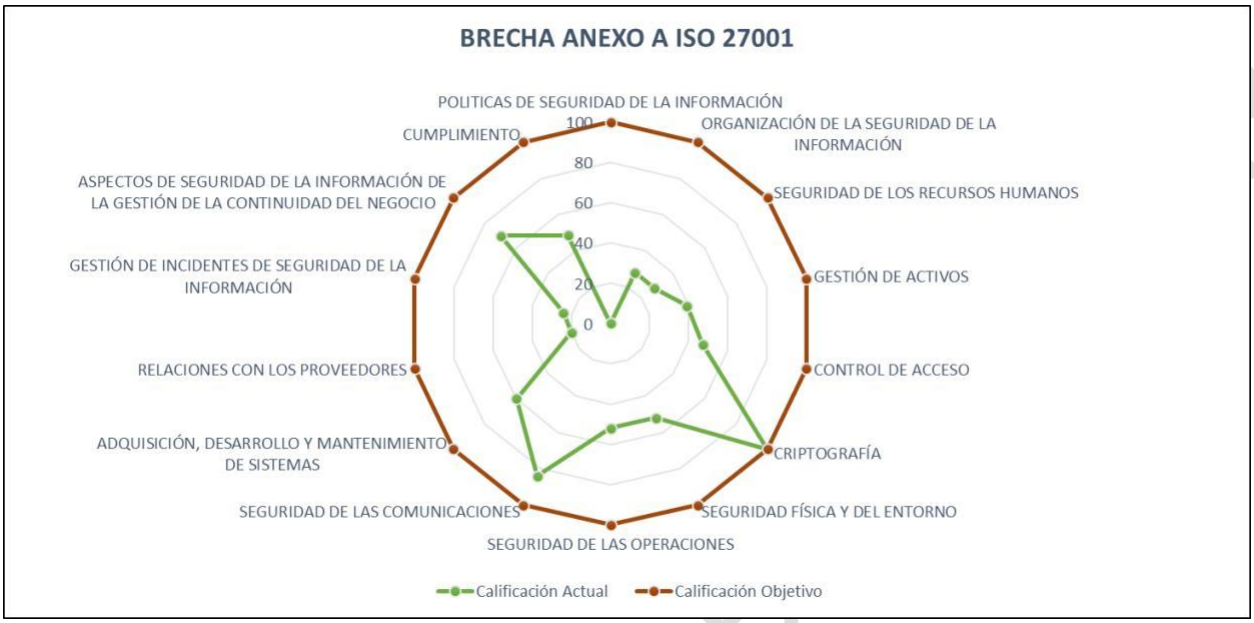
		problema y que hay que tratarlo. • No hay procesos estandarizados. • La implementación de un control depende de cada individuo y es principalmente reactiva. • Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	• Los procesos y los controles son un patrón regular. • Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. • No hay formación ni comunicación formal sobre los procedimientos y estándares. • Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	• Los procesos y los controles se documentan y se comunican. • Los controles son efectivos y se aplican casi siempre; 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.
Gestionado	80	• Los controles se monitorean y se miden. • Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	• Las buenas prácticas se siguen y automatizan. • Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Resultados

Tomando como base la escala de valoración anterior, se realizó el entendimiento y análisis de la documentación y procedimientos existentes para posteriormente asignar una calificación a cada uno de los controles según los dominios evaluados, obteniendo los siguientes resultados:

- **Brecha Anexo A ISO 27001**

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	0 INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	28	100	2 REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	28	100	2 REPETIBLE
A.8	GESTIÓN DE ACTIVOS	39	100	2 REPETIBLE
A.9	CONTROL DE ACCESO	47	100	3 EFECTIVO
A.10	CRIPTOGRAFÍA	100	100	5 OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	52	100	3 EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	52	100	3 EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	84	100	5 OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	100	3 EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	20	100	1 INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	24	100	2 REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	4 GESTIONADO
A.18	CUMPLIMIENTO	48,5	100	3 EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**47**	**100**	3 EFECTIVO



Observaciones: Los resultados de la evaluación de efectividad de los controles indican un panorama mixto en cuanto a la implementación de las medidas de seguridad de la información. En general, la Universidad se encuentra en una etapa incipiente en la adopción del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) en su operación cotidiana.

Algunos dominios muestran un grado de madurez en la implementación de controles, siguiendo un patrón repetible pero que aún no es completamente estable, lo que indica un progreso en la implementación de medidas de seguridad, pero también resalta la necesidad de mejoras significativas para alcanzar los estándares deseados.

De manera general la calificación global actual de la Universidad del Cauca en cuanto a la **efectividad de los controles de seguridad de la información es de 47 sobre 100.** Se identifican áreas clave que requieren mejoras, lo que enfatiza la necesidad de enfocar los esfuerzos hacia la mejora continua en seguridad de la información y el fortalecimiento de los estándares internos.

Nota: Para cada control evaluado, se registraron observaciones que permiten un mejor entendimiento de la situación. Dichas observaciones se encuentran disponibles en el Instrumento de Evaluación del MSPI.

- **Avance PHVA**

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual	% Avance Esperado
2023	Planificación	9%	40%
	Implementación	5%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		14%	100%

Observaciones: Se ha evaluado el progreso del ciclo PHVA como parte del proceso de implementación del SGSI. Este ciclo PHVA es esencial para la gestión efectiva de la seguridad de la información.

Se destaca que aunque se ha logrado cierto avance en cada componente, en general, el progreso actual se encuentra en un 14% en comparación con el objetivo esperado del 100%.

Estos resultados subrayan la importancia de fortalecer el compromiso y los esfuerzos en todas las etapas del ciclo PHVA para garantizar una implementación exitosa del SGSI en la Universidad del Cauca.

- **Nivel de Madurez**

		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	INTERMEDIO
	Repetible	INTERMEDIO
	Definido	INTERMEDIO
	Administrado	CRÍTICO
	Optimizado	CRÍTICO

Observaciones: El análisis general de la Seguridad y Privacidad de la Información en la Universidad del Cauca revela un panorama en evolución de acuerdo a los niveles de madurez del MSPI (MinTIC), que van desde “Inicial” hasta “Optimizado”. Estos niveles reflejan el grado de desarrollo de los controles y procesos de seguridad de la información en la institución.

La universidad se encuentra posicionada principalmente entre los niveles de madurez “Repetible” e “Intermedio”.

- En el nivel “Repetible”, se identifica que se han establecido procesos básicos de gestión de la seguridad, y existen algunos controles para detectar posibles incidentes de seguridad, aunque no están completamente integrados en toda la operación de la universidad.

- En el nivel “Intermedio” la universidad demuestra avances en la documentación de procesos, lineamientos y controles de Seguridad y Privacidad de la Información, pero se requiere un esfuerzo mayor para lograr la estandarización e institucionalización, y con ello mejorar la implementación y efectividad de los procesos, lineamientos y controles.

Es importante destacar que los niveles superiores “Administrado” y “Optimizado” se identifican como “críticos”, esto indica que la universidad enfrenta desafíos significativos en la gestión de la Seguridad y Privacidad de la Información, y actualmente no cumple con los requisitos establecidos para posicionarse en estos niveles. Es fundamental que la universidad tome medidas relevantes para mejorar sus prácticas y elevar su nivel de madurez en estos aspectos.

De manera general, la Universidad del Cauca ha logrado cierto grado de madurez en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), pero se enfrenta a desafíos importantes en términos de efectividad y sistematización de los controles. Se recomienda una revisión exhaustiva y medidas correctivas urgentes para elevar el nivel de madurez en estos aspectos críticos y avanzar hacia niveles de cumplimiento más altos.

Anexos relacionados:

- Instrumento de evaluación MSPI.xlsx
- Informe de diagnóstico – Enero 2024.pdf

7. Fase 1: Planificación

7.1. Contexto

7.1.1. Comprensión de la organización y de su contexto

Perfil de la Universidad

La Universidad del Cauca, establecida en 1827, es una institución pública de educación superior en Colombia. Destaca en la formación académica, la investigación y la extensión social, ofreciendo una

variedad de programas en ciencias, ingeniería, salud, humanidades, y artes. Su compromiso se centra en generar conocimiento, promover la cultura y contribuir al desarrollo regional y nacional. La Universidad se esfuerza por ser un referente en innovación educativa y un agente de cambio social, fomentando un ambiente inclusivo y dinámico para su comunidad académica y estudiantil.

Contexto estratégico

En el marco del Plan de Desarrollo Institucional 2023-2027, la Universidad del Cauca está realizando pasos significativos para fortalecer su infraestructura y políticas en áreas clave. Con un enfoque en la calidad académica y la integración tecnológica, la universidad ha implementado estrategias importantes para alinear sus operaciones con los desafíos y oportunidades del siglo XXI. Entre estas estrategias, destacan:

1. **Plan de Desarrollo Institucional 2023-2027:** Enfocado en mejorar la calidad educativa y la investigación.

2. **Implementación del PETI 2023-2027 (Plan Estratégico de Tecnología):** Modernización de la infraestructura tecnológica y procesos de la universidad.

3. **Desarrollo del SGSI 2024-2027 (Sistema de Gestión de Seguridad de la Información):** Fortalecimiento de la Seguridad y Privacidad de la Información, basado en ISO 27001 y el MSPI definido por el MinTIC.

Este enfoque estratégico no solo cumple con los objetivos actuales de la Universidad del Cauca, sino que también establece una base sólida para su futuro desarrollo, asegurando que la institución siga siendo un referente en el ámbito educativo y tecnológico.

7.1.2. Necesidades y expectativas de los interesados

Para definir el **Plan de Seguridad y Privacidad de la Información** (vigente hasta 2027), la Universidad del Cauca llevó a cabo un proceso detallado de levantamiento de información. Los hallazgos de este proceso se han organizado en una matriz de necesidades y expectativas, que se encuentra en el **Anexo 1 – Matrices del SGSI.xlsx.**

Esta matriz es la base del plan, y no sólo guía la implementación de medidas de seguridad, sino que también permite definir prioridades y objetivos claros.

Reconociendo el entorno cambiante de la seguridad de la información, la universidad actualizará esta matriz y el plan estratégico asociado anualmente. Este enfoque garantiza que nuestra estrategia se mantenga relevante frente a las nuevas tecnologías, amenazas de seguridad y requerimientos legales.

7.1.3. Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad tiene aplicabilidad y alcance sobre todas las áreas, procesos, sistemas, y miembros de la comunidad universitaria, asegurando una cobertura integral en la protección y gestión de la información.

- **Cobertura Institucional:** El SGSI se aplica a todas las facultades, departamentos, y unidades administrativas de la Universidad, incluyendo sedes centrales y regionales.
- **Comunidad Universitaria:** El SGSI es aplicable a todos los miembros de la Universidad, incluyendo estudiantes, docentes, personal administrativo y de apoyo, así como a contratistas y terceros que interactúen con los sistemas de información de la institución.
- **Cumplimiento Normativo y Legal:** El alcance del SGSI también abarca el cumplimiento de normatividad pertinente a nivel nacional e internacional relacionadas con la Seguridad de la Información y la protección de datos.

Nota importante: El **documento maestro del SGSI** es un artefacto vivo, sujeto a evaluaciones y mejora continua, adaptándose a los cambios en el entorno tecnológico, las amenazas de seguridad emergentes y las necesidades cambiantes de la Universidad.

7.1.4. Componentes del SGSI de la Universidad del Cauca

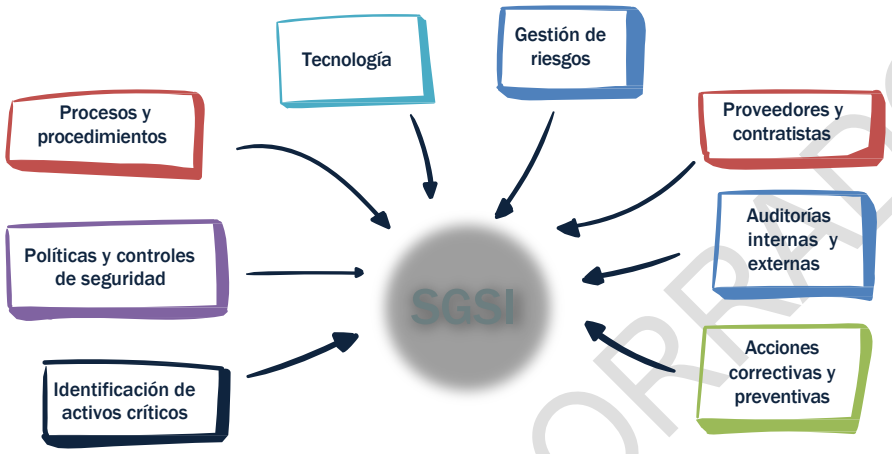


Ilustración 1 - Componentes del SGSI de la Universidad del Cauca

- **Identificación de activos críticos:** Incluye la identificación de todos aquellos activos que son vitales para la misionalidad de la Universidad y requieren protección especial y/o adicional. Esto cubre todos los datos y la información generados, almacenados, procesados y transmitidos por la Universidad, abarcando desde datos personales de estudiantes y funcionarios, hasta información de investigación, académica, financiera y administrativa.

- **Políticas y controles de seguridad:** Incluye la política general de seguridad y privacidad de la información de la Universidad, el manual de políticas y todas las directrices que se establezcan para mantener la seguridad y la privacidad de la información.

- **Procesos y procedimientos:** Se incluyen todos los procesos y procedimientos relacionados con la gestión de la Seguridad y Privacidad de la Información, desde el acceso y uso de los sistemas de información hasta su mantenimiento, protección y disposición final.

- **Tecnología:** Se refiere a las herramientas, infraestructura tecnológica y sistemas de información que se utilizan para proteger la información y garantizar la seguridad de la información en la universidad. El SGSI cubre toda la infraestructura tecnológica de la Universidad, incluyendo redes, sistemas, bases de datos, plataformas digitales, equipos de cómputo y cualquier otro recurso tecnológico utilizado en el procesamiento y almacenamiento de información.

- **Gestión de Riesgos:** Incluye la identificación, análisis, tratamiento y monitoreo de riesgos relacionados con la Seguridad de la Información, así como la preparación y respuesta ante incidentes de seguridad.

- **Proveedores y contratistas:** Incluye el manejo de las relaciones con terceros que tienen acceso o impactan la seguridad de la información, asegurando que se adhieran a las políticas de seguridad establecidas.

- **Auditorías internas y externas:** Son las evaluaciones regulares del SGSI para asegurar la conformidad con los estándares de seguridad y detectar oportunidades de mejora.

- **Acciones correctivas y preventivas:** Incluye todas las medidas tomadas para corregir y prevenir incidentes de seguridad de la información.

7.2. Liderazgo

7.2.1. Liderazgo y Compromiso

La Universidad del Cauca reconoce que el liderazgo efectivo y el compromiso genuino de todas las partes interesadas son fundamentales para el éxito de la Seguridad y Privacidad de la Información. En este sentido, y con el fin de garantizar un correcto liderazgo, se formula una **resolución** que amplía las responsabilidades del **Comité Institucional de Gestión del Desempeño y de Control Interno**, marcando un hito importante en el camino hacia una gestión más robusta y consciente de la Seguridad y Privacidad de la Información.

Este Comité, respaldado por la alta dirección, asume la responsabilidad de liderar la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Por otra parte, reconociendo la importancia crítica de la tecnología en la misión institucional, el liderazgo de la **División TIC** también juega un papel vital en la promoción de prácticas seguras y privadas en el uso de la información y los sistemas de información.

Al fortalecer el liderazgo y fomentar un compromiso profundo con la Seguridad y Privacidad de la Información, la Universidad del Cauca busca asegurar que sus esfuerzos asociados a la transformación digital y manejo de la información se ejecuten dentro de un entorno seguro, respetuoso con la privacidad y alineado con sus metas estratégicas y valores institucionales.

Nota de alcance: El liderazgo en la Seguridad y Privacidad de la Información se extiende a través de la asignación de responsabilidades específicas dentro de diversas oficinas y divisiones de la Universidad, donde cada actor desempeña un rol crucial en la protección de la información. Los detalles de estas asignaciones se especifican en la sección de Roles y Responsabilidades del presente documento maestro (sección 7.2.3).

7.2.2. Política de seguridad y privacidad de la información

La Universidad del Cauca ha reconocido, a lo largo de su historia, la importancia de proteger la información como un activo esencial para el cumplimiento de su misión institucional. En este marco, la **Resolución R-785 de 2015** estableció la **Política del Sistema de Gestión de Seguridad de la Información**, sentando las bases para una gestión consciente y estructurada de la seguridad de la información.

Reconociendo la necesidad de adaptarse a los desafíos cambiantes de seguridad y privacidad en el entorno digital, la Universidad ha dado un paso adelante con la expedición de un nuevo acto administrativo. Esta actualización no solo clarifica y refuerza la política existente, sino que también incorpora un nuevo **Manual de política de Seguridad y Privacidad de la Información**, establece formalmente el Sistema de Gestión

de Seguridad de la Información (SGSI) en la Universidad del Cauca, y define las responsabilidades frente a la Seguridad y Privacidad de la Información.

La actualización de la política de seguridad refleja el compromiso de la Universidad con la mejora continua y la privacidad de la información, asegurando que las estrategias y prácticas de gestión de la información estén alineadas con los estándares internacionales más actuales y respondan de manera efectiva a los riesgos emergentes. Además, la actualización a esta política fortalece la integración de la seguridad y privacidad en todos los niveles de la institución, promoviendo una cultura de responsabilidad y conciencia entre estudiantes, docentes y personal administrativo.

Anexos relacionados

- Manual de políticas de seguridad y privacidad de la información.pdf

7.2.3. Roles y responsabilidades

Para lograr el fortalecimiento de la Seguridad y Privacidad de la Información en la Universidad, se requiere la participación y el compromiso de diversos roles y responsabilidades. Para ello, es fundamental definir claramente estos roles y responsabilidades, así como formalizar su asignación a través de los mecanismos administrativos correspondientes. A continuación, se presenta un resumen de los roles y responsabilidades clave en materia de seguridad de la información definidos por la Universidad:

- **Comité Institucional de Gestión del Desempeño y de Control Interno:** Representa la alta dirección y es el organismo máximo en la toma de decisiones estratégicas relacionadas con el SGSI en la Universidad del Cauca.
- **Contratación del Oficial de Seguridad y Privacidad de la Información (Equivalente a un Chief Information Security Officer - CISO para la Universidad):** Existe una iniciativa para contratar a un rol responsable de la Seguridad y Privacidad de la Información en la Universidad. Este rol se encargaría de coordinar la implementación, mantenimiento y mejora continua del SGSI. Sin

embargo, al momento de la definición del presente documento maestro (2024) aún existen varios trámites administrativos pendientes para lograr esta contratación, es por ello por lo que la División TIC proveerá temporalmente el personal técnico que pueda suplir parte de las responsabilidades y se asegure la continuidad del SGSI.

- **Contratar los servicios de Auditoría Externa en Seguridad y Privacidad de la Información:** Son empresas o personas expertas en la realización de auditorías independientes contratadas para evaluar la efectividad del SGSI y proporcionar recomendaciones de mejora, además de realizar pruebas de vulnerabilidades a los sistemas de información. Es importante aclarar que estos servicios no son permanentes y se contratan de forma anual para mantener la robustez tecnológica en materia de seguridad.

Las siguientes áreas de la Universidad (ya existentes) también aportan al tema de la seguridad de la información, por tal motivo se realizó la socialización de las responsabilidades de las oficinas o formalización de responsabilidades en materia de Seguridad y Privacidad de la Información para:

- **Oficina Asesora Jurídica:** Brindar asesoría legal en temas de Seguridad y Privacidad de la Información, incluyendo la gestión de incidentes, contratos y acuerdos de confidencialidad.
- **Oficina de Control Interno:** Realizar auditorías internas, evalúa la efectividad de las políticas de seguridad y participa en la gestión de riesgos de seguridad de la información.
- **División de Gestión del Talento Humano:** Responsables de la capacitación, concienciación y cumplimiento de las políticas de seguridad por parte del personal.
- **Centro de Gestión de las Comunicaciones:** Apoya la divulgación y concienciación en seguridad de la información a través de los canales de comunicación institucionales.
- **Centro de Gestión de la Calidad:** Garantiza la alineación del SGSI con el Sistema de Gestión de Calidad y promueve la mejora continua.

- **División Administrativa y de Servicios:** Gestiona la seguridad física, el mantenimiento de la infraestructura y la administración del ciclo de vida de los dispositivos tecnológicos.
- **Oficina Asesora de Planeación:** Incorpora objetivos de seguridad de la información en la planeación institucional y asigna recursos para la implementación y mejora del SGSI.
- **Área de Gestión Documental (Secretaría General):** Gestiona la seguridad de la información documentada, incluyendo la clasificación, retención y disposición de los activos de información.

Otras responsabilidades

- **Creación del Equipo técnico para la seguridad digital (Interno de la División TIC):** Existe la iniciativa para que la **División TIC**, forme un equipo encargado de la protección de los recursos tecnológicos de la Universidad del Cauca. Formado por coordinadores de distintas áreas de la **División TIC**, este equipo multidisciplinario es responsable de establecer y mantener los mecanismos de defensa de la infraestructura de TI. Además de tomar decisiones, definir planes y estrategias para asegurar los recursos tecnológicos de la Universidad.

Nota: El detalle de las actividades específicas de cada involucrado en la Seguridad y Privacidad de la información está disponible en **Anexo 2 - Roles y responsabilidades en Seguridad de la Información.pdf**

7.3. Planificación y gestión de riesgos

7.3.1. Identificación de activos de seguridad digital (activos de información e infraestructura crítica)

Nota de alcance: Para esta sección se sugiere manejar los conceptos de “activos de información e infraestructura crítica”, sin embargo, con el fin de asegurar la alineación con la **Metodología para la**

División de las Tecnologías de la Información y las Comunicaciones
Carrera 3 No. 3N-51 - Sector Tulcán Popayán - Cauca – Colombia
Teléfono: 8209842 Conmutador 8209800
jefaturatic@unicauca.edu.co - www.unicauca.edu.co

administración del riesgo de la Universidad del Cauca - MARUC, se adopta el concepto de "activo de seguridad digital".

Identificar los activos de seguridad digital constituye un pilar fundamental para empezar a establecer la estrategia de Seguridad y Privacidad de la Información en la Universidad. Esta actividad toma gran importancia no solo por la relevancia de reconocer los activos que son esenciales para el funcionamiento académico y administrativo, sino que también permite demarcar las responsabilidades y aplicar estrategias de protección adecuadas a cada tipo de activo.

En este contexto, resulta crucial aclarar que los activos de seguridad digital se clasifican en "activos de información física", los cuales incluyen documentos y registros en formatos físicos (como contratos, comunicados, informes, etc.); y "activos de información digital", que incluyen los recursos tecnológicos de la Universidad.

Debido a esta distinción, se identifican responsabilidades específicas en el tratamiento de estos activos: para los activos de información general, la responsabilidad de su gestión recae en el **Área de Gestión Documental**, mientras que, la gestión de la infraestructura crítica tecnológica es responsabilidad directa de la **División TIC**, tal y como se relaciona a continuación:

- El **Área de Gestión Documental** es responsable de la catalogación de los activos de información física de la Universidad, asegurando su adecuada protección y acceso en conjunto con el área de Archivo central, siguiendo los lineamientos del Acuerdo Superior 074 de 2020 (Por el cual se adopta la Política de Gestión Documental de la Universidad del Cauca).

- La **División TIC** tiene la responsabilidad de identificar y gestionar los activos de información digital, que corresponde a los servidores, redes de datos, sistemas de información y bases de datos, los cuales resultan vitales para mantener la operación de la Universidad; y para ello se define un procedimiento específico para la **División TIC** alineado con la **Metodología para la administración del riesgo de la Universidad del Cauca - MARUC**, el cual cubre actividades clave como: Mantener

un inventario actualizado de los activos de información digital; clasificar estos activos según su criticidad e impacto para la operación de la Universidad; identificar y aplicar medidas de protección adecuadas para mitigar vulnerabilidades; y monitorear las medidas de protección para garantizar su efectividad continua y ajustarlas según sea necesario.

Nota: el detalle de este procedimiento se encuentra en el anexo **Procedimiento de Identificación, clasificación y protección de activos tecnológicos críticos.pdf**

7.3.2. Valoración de los riesgos de seguridad de la información

La Universidad del Cauca reconoce la importancia de contar con un proceso meticuloso de valoración de riesgos en Seguridad y Privacidad de la Información como punto de partida crucial para la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI). El enfoque de este proceso debe estar alineado con las directrices del MinTIC e incluir la identificación, análisis, valoración y tratamiento de riesgos, asegurando un monitoreo y revisión constantes, facilitando así la toma de decisiones informadas y la aplicación de los controles apropiados.

En este contexto, la **"Metodología para la Administración del Riesgo de la Universidad del Cauca – MARUC"**, articulada por la Oficina de Planeación, provee un marco sistemático y preventivo para la gestión de riesgos alineado con la legislación nacional e internacional, y con prácticas estandarizadas de gestión de riesgo. Esta metodología se incorpora a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) manteniendo la alineación con los objetivos misionales y estratégicos de la Universidad.

Nota: el detalle de la "Metodología para la Administración del Riesgo de la Universidad del Cauca – MARUC" se encuentra en el **Anexo PV-GC-2.6-OD-03 Metodología para la Administración del Riesgo de la Universidad del Cauca:**

https://facultades.unicauca.edu.co/prlvmen/sites/default/files/procesos/PE-GE-2.4-OD-5%20Gu%C3%ADa%20Metodol%C3%B3gica%20Gesti%C3%B3n%20del%20Riesgo%20MARUC%20V2.pdf

7.3.3. Plan de tratamiento de los riesgos de seguridad de la información

El **Plan de Tratamiento de los Riesgos de Seguridad y Privacidad** de la Información es un documento detallado que se desarrolla de forma independiente a este documento maestro. Este plan específico aborda las estrategias y medidas adoptadas para gestionar los riesgos identificados durante la evaluación de seguridad de la información, asegurando así la protección y confidencialidad de los datos manejados por la Universidad del Cauca. El plan incluye la identificación de amenazas, la valoración de vulnerabilidades, y las acciones correspondientes para mitigar o aceptar cada riesgo según la política de seguridad de la institución. Para una comprensión integral y actualizada de las prácticas y procedimientos adoptados en materia de seguridad de la información, se recomienda consultar el **Plan de Tratamiento de los Riesgo de Seguridad y Privacidad de la Información** específico.

Anexos relacionados

- Plan de Tratamiento de los Riesgo de Seguridad y Privacidad de la Información.pdf

7.4. Habilitadores del SGSI (Soporte)

7.4.1. Recursos (financieros, humanos y técnicos)

La Universidad del Cauca, consciente de la importancia del Sistema de Gestión de Seguridad de la Información (SGSI), reconoce la necesidad de asignar recursos adecuados para su adopción efectiva. Esto se considera esencial, dado que el SGSI es un sistema transversal que involucra a toda la institución, y como tal, requiere de una estrategia integrada que abarque diversos ámbitos de actuación.

Para mantener en marcha el SGSI y asegurar su relevancia y efectividad constantes, la Universidad se compromete a destinar los recursos financieros, humanos, tecnológicos y cualquier otro recurso necesario que permita la adecuada adopción, implementación, mantenimiento y mejora continua del sistema, integrando así la seguridad y la privacidad en el núcleo de nuestras operaciones institucionales.

Tomando como base el **Plan de Desarrollo Institucional 2023-2027** y los proyectos de inversión en tecnología, se han identificado y asignado los siguientes recursos para el establecimiento del SGSI:

Recursos financieros:

Nota de alcance: La **División TIC**, al definir el SGSI y estar al frente de los esfuerzos de implementación, gestionará los recursos financieros iniciales destinados a la seguridad. Con el objetivo de ampliar el alcance del SGSI más allá de las TIC y abarcar toda la institución, se evaluará la posibilidad de asignar un presupuesto específico para la Seguridad y Privacidad de la Información desde un nivel institucional, con miras a mantener operativo el Sistema de Gestión de Seguridad de la Información (SGSI) de carácter transversal.

Se espera destinar entre el 10% y 15% del presupuesto anual de la **División TIC** (aprox. $154-$230 millones de pesos colombianos para 2024) para la implementación de iniciativas específicas relacionadas con el SGSI, tales como adquisición de soluciones de seguridad, licenciamiento, servicios de consultoría especializada, realización de diagnósticos / pruebas de seguridad, actividades de capacitación y, de ser necesario, la contratación de personal especializado.

Paralelamente, en los proyectos de inversión tecnológica ya aprobados y en marcha se destinan rubros específicos para fortalecer la seguridad física, actualización de sistemas de información existentes y renovación de licencias.

Nota: Es importante señalar que, dado que el **Plan de Desarrollo Institucional 2023-2027** y los proyectos de inversión iniciales no desglosan de manera explícita los fondos destinados a seguridad, la asignación de estos recursos está sujeta a variaciones en función de las necesidades reales de la Universidad y la

disponibilidad presupuestaria, por lo que el porcentaje final podría ser ajustado, ya sea incrementándose o reduciéndose, para adaptarse a los objetivos estratégicos de la Universidad y a las dinámicas del contexto operativo.

Recursos humanos:

Nota de alcance: Actualmente, la Universidad del Cauca es consciente de la necesidad crítica de incorporar un profesional especializado que lidere las operaciones del SGSI. Reconociendo este requisito, la contratación de tal perfil es una meta pendiente, condicionada a factores estructurales y organizativos, incluyendo posibles reestructuraciones que permitan una integración efectiva del rol dentro de la institución.

Entre tanto, y para no desatender las necesidades del SGSI, la Universidad está comprometida a aprovechar la experticia del personal existente, aprovechando su conocimiento previo en temas técnicos y en normativas como la ISO 27001:2022.

Como solución provisional y para garantizar una implementación adecuada del sistema, se están ajustando las responsabilidades del personal actual y redefiniendo la estructura de los comités correspondientes, tal como se describe en la **sección 7.2.3** de este documento. Estas medidas temporales son pasos proactivos para habilitar la seguridad de la información, sin que la espera por un nuevo especialista constituya una barrera para la operación efectiva del SGSI.

Recursos tecnológicos:

Dentro del contexto del **Plan de Desarrollo Institucional 2023-2027** y los esfuerzos de la **División TIC** para establecer y mantener el SGSI, se contempla la evaluación y mejoramiento de la infraestructura tecnológica, una iniciativa que ya se encuentra incorporada de forma transversal en los cuatro proyectos clave definidos por la **División TIC**:

1. Modernización de recursos y plataformas tecnológicas

2. Modernización del portal web institucional

3. Fortalecimiento de procesos académico-administrativos a través de la implementación de un Sistema de Gestión integral

4. Modernización de comunicaciones - telefonía VoIP

Adicionalmente se contempla la adquisición de soluciones de almacenamiento de copias de seguridad y control de acceso físico (facultades, sedes administrativas y centros de cableado).

Como parte de la operación, están asegurados los recursos para renovar los certificados de seguridad, licencias y soportes de plataformas críticas.

Además, se mantendrá un compromiso con la mejora continua de la infraestructura tecnológica ya existente, asegurando su adaptación y evolución constante para responder a los desafíos emergentes de Seguridad y Privacidad de la Información.

Nota: Se realizará seguimiento riguroso por parte de la **División TIC** a la asignación de recursos y ejecución de las iniciativas planteadas en la hoja de ruta (a través de la plataforma **Gesthor ITSM https://unicauca.gesthor.me**) con el fin de hacer los ajustes necesarios en futuros ejercicios presupuestarios, esto para garantizar el soporte continuo al SGSI, de acuerdo con las necesidades de la Universidad y asegurando la alineación con los objetivos del **Plan de Desarrollo Institucional 2023-2027** y objetivos de seguridad de la información.

Anexos relacionados: Anexo 1 – Matrices del SGSI.xlsx

7.4.2. Competencia, toma de conciencia y comunicación

La Universidad del Cauca, como parte de su compromiso con la mejora continua, ha decidido promover las siguientes estrategias que permitan habilitar la adopción de buenas prácticas e impulsar la cultura de seguridad:

- Plan de comunicación y gestión del cambio

Estas estrategias están diseñadas para cubrir el **Plan Estratégico de Tecnologías de la Información (PETI)**, la formalización del Sistema de Gestión de Seguridad de la Información (SGSI), y las iniciativas del recientemente establecido **Equipo de Gestión del Cambio** de la División de Tecnologías de la Información y las Comunicaciones (TIC).

Estas estrategias buscan garantizar una comunicación coherente y sinérgica para toda la comunidad universitaria, optimizando recursos y asegurando que los mensajes clave sean consistentemente reforzados.

En lo que respecta específicamente al componente de Seguridad y Privacidad de la Información, estas estrategias tendrán como objetivos principales:

1. Garantizar que los interesados clave de la Universidad, incluyendo directivos, docentes, administrativos y estudiantes, cuenten con los conocimientos, habilidades y conciencia necesarios para contribuir a la implementación exitosa y la sostenibilidad del SGSI.

2. Promover una cultura de Seguridad y Privacidad de la Información en toda la comunidad universitaria, que trascienda el ámbito puramente tecnológico y se integre en las actividades cotidianas y los procesos clave de la Universidad.

3. Establecer canales de comunicación efectivos para mantener informados a los distintos actores sobre los avances, requisitos y responsabilidades relacionados con la Seguridad y Privacidad de la Información, así como para recibir retroalimentación y promover la participación.

4. Generar conciencia sobre los riesgos asociados a la seguridad de la información y la importancia de aplicar buenas prácticas y en consecuencia ajustar el comportamiento para mitigar dichos riesgos, tanto en el contexto laboral como personal.

Para desarrollar las estrategias y alcanzar estos objetivos, se contemplan las siguientes acciones:

- Desarrollar un plan de capacitación y sensibilización continua, considerando las necesidades y conocimiento de los diferentes actores dentro de la Universidad. Se aprovechará la infraestructura y recursos de aprendizaje existentes, como la plataforma virtual institucional (https://univirtual.unicauca.edu.co/moodle/login/index.php), para facilitar el acceso y la participación.

- Fomentar la integración de los principios y prácticas de seguridad de la información en los programas de inducción para nuevos empleados y estudiantes, así como en los procesos de crecimiento profesional dentro de la Universidad.

- Ejecutar campañas periódicas de sensibilización, a través de diversos medios como correo electrónico, redes sociales institucionales, eventos presenciales y virtuales (alineados con los esfuerzos del **Proyecto de Apropiación Tecnológica - PROTEO**), entre otros, para que la comunidad universitaria comprenda la importancia de dar un tratamiento adecuado a la información.

- Medir periódicamente los niveles de apropiación y aplicación de las políticas y prácticas de seguridad, a través de encuestas, evaluaciones, medición de cantidad de incidentes de seguridad y otros mecanismos de retroalimentación, cuyos resultados servirán para ajustar y mejorar continuamente el plan.

Nota: La Universidad del Cauca asignará los recursos necesarios para el diseño, ejecución y seguimiento de estas estrategias (Plan de comunicación y gestión del cambio - Plan de capacitación y sensibilización), como parte integral de los esfuerzos dedicados a la implementación del SGSI, y velará por su alineación con los objetivos institucionales y las necesidades de la comunidad universitaria.

Anexos relacionados: Anexo 1 – Matrices del SGSI.xlsx

8. Fase 2: Operación

8.1. Implementación

En la Universidad del Cauca, entendemos que la implementación efectiva del Sistema de Gestión de Seguridad de la Información (SGSI) es crucial para proteger nuestros activos digitales y asegurar la confidencialidad, integridad, y disponibilidad de nuestra información.

Esta fase de implementación del SGSI tiene como propósito fundamental traducir la estrategia de seguridad de la información en acciones concretas y efectivas, esto a través de la definición y ejecución de un plan de acción detallado, factible y alineado con los recursos disponibles, que permita implementar los controles de seguridad y todas las iniciativas y proyectos necesarios para dar tratamiento a los riesgos identificados y cumplir con los requisitos del SGSI; dichos controles están basados en los 93 controles de seguridad definidos en la norma ISO/IEC 27001:2022, que a su vez son el corazón del manual de políticas de Seguridad y Privacidad de la Información.

Estos controles se organizan en cuatro categorías principales: controles organizacionales (37), controles sobre personas (8), controles físicos (14) y controles tecnológicos (34), abarcando así todos los aspectos clave de la seguridad de la información.

Es importante resaltar que la implementación de estos controles representa un gran paso en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Universidad del Cauca, sentando las bases para su potencial integración con el Sistema de Gestión de Calidad certificado bajo la norma ISO 9001.

La **División de Tecnologías de la Información y las Comunicaciones (TIC)** por su parte mantiene una hoja de ruta dinámica en la plataforma **Gesthor ITSM**, la cual recopila y prioriza los proyectos estratégicos relacionados con la seguridad de la información y la infraestructura tecnológica. Estos proyectos están alineados con los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) y buscan fortalecer continuamente la postura de seguridad de la universidad.

La hoja de ruta abarca diversos aspectos, tales como:

- Renovación y actualización de licencias de software crítico para la seguridad y el funcionamiento de los sistemas.
- Evaluación continua de vulnerabilidades y amenazas, incluyendo la realización de pruebas de penetración en plataformas y portales críticos.
- Mejoras en los controles de acceso físico y lógico.
- Fortalecimiento de la seguridad en la infraestructura de red, incluyendo la configuración de funcionalidades de seguridad.
- Formalización y contratación de roles específicos para la gestión de la seguridad de la información.
- Aprobación, publicación y mantenimiento de políticas, procedimientos y documentos relacionados con el SGSI y el Plan Estratégico de Tecnologías de la Información (PETI).
- Integración del SGSI con otros sistemas de gestión, orientado a la certificación ISO 27001:2022.
- Evaluación y aplicación de controles del Manual de Políticas del SGSI.
- Desarrollo de lineamientos para el desarrollo seguro y la experiencia de usuario (UX).
- Apoyo a trabajos de grado relacionados con la gestión de incidentes de seguridad, gestión de problemas, gestión de configuración y procedimientos seguros de inicio de sesión.

- Desarrollo e implementación de planes de continuidad del negocio y recuperación ante desastres.
- Modernización de sistemas de información misionales.
- Estudio de viabilidad para la implementación de tecnologías de seguridad adicionales

Nota: El plan detallado de implementación del SGSI se encuentra documentado y resguardado en la plataforma **Gesthor ITSM** de la Universidad, accesible para el equipo responsable de su ejecución, esto debido al nivel de **confidencialidad** necesario en este plan. Para más información sobre las acciones y estrategias específicas adoptadas, invitamos a nuestra comunidad universitaria a contactar directamente con la **División TIC**, quienes facilitarán los detalles pertinentes y responderán a cualquier consulta relacionada.

Anexos relacionados:

- Plan de implementación en plataforma - Gesthor ITSM (https://unicauca.gesthor.me)
- Plan de tratamiento de riesgos en plataforma Gesthor ITSM (https://unicauca.gesthor.me)
- Gestión de riesgos en plataforma Gesthor ITSM (https://unicauca.gesthor.me)
- Manual de políticas de seguridad y privacidad de la información.pdf

9. Fase 3: Evaluación de desempeño

9.1. Seguimiento, medición, análisis y evaluación

La Universidad del Cauca cuenta con mecanismos robustos para el seguimiento, medición, análisis y evaluación del desempeño del Sistema de Gestión de Seguridad de la Información (SGSI). Esto gracias a un conjunto de métricas e indicadores clave que permiten evaluar la efectividad de los controles implementados, el cumplimiento de los objetivos de seguridad y la identificación de oportunidades de mejora.

El seguimiento se realiza de manera periódica, con una frecuencia definida según la criticidad de cada control y proceso. Los resultados son documentados y analizados por el equipo responsable del SGSI, quienes reportan los hallazgos relevantes al **Comité Institucional de Gestión del Desempeño y de Control Interno.**

Además, se llevarán a cabo evaluaciones de riesgos regulares para identificar cambios en el contexto interno y externo de la Universidad que puedan afectar la seguridad de la información, y se ajustarán los controles y planes de tratamiento en consecuencia.

9.2. Auditoría Interna

La Universidad del Cauca cuenta con un programa de auditorías internas para evaluar de manera objetiva e independiente la conformidad del SGSI con los requisitos de la norma ISO/IEC 27001, las políticas y procedimientos internos, y los requisitos legales y reglamentarios aplicables.

Las auditorías son planificadas y ejecutadas por la **Oficina de Control Interno y la División TIC**, y de forma externa a la Universidad gracias a la contratación de servicios de empresas líderes en el sector. Los resultados de las auditorías, incluyendo las no conformidades y oportunidades de mejora identificadas, serán reportados al **Comité Institucional de Gestión del Desempeño y de Control Interno** para su revisión y la toma de acciones correctivas y preventivas.

Anexos relacionados:

- **Manual de políticas de seguridad y privacidad de la información.pdf**
- **Anexo 1 – Matrices del SGSI.xlsx**

9.3. Revisión por la dirección

La alta dirección de la Universidad del Cauca (representada por el **Comité Institucional de Gestión del Desempeño y de Control Interno**), con el apoyo de la **Oficina de Control Interno**, llevará a cabo revisiones periódicas del SGSI para asegurar su conveniencia, adecuación y eficacia continuas. Estas revisiones considerarán:

- El estado de las acciones de revisiones previas.
- Los cambios en las cuestiones externas e internas relevantes para el SGSI.
- La retroalimentación sobre el desempeño de la seguridad de la información, incluyendo tendencias en no conformidades, acciones correctivas, resultados de seguimiento y medición, y resultados de auditoría.
- Las oportunidades de mejora continua.

Los resultados de la revisión incluirán decisiones y acciones relacionadas con las oportunidades de mejora, cualquier necesidad de cambio en el SGSI y las necesidades de recursos. Estos resultados serán documentados y comunicados a las partes interesadas relevantes.

10. Fase 4: Mejoramiento continuo

10.1. Mejora

La Universidad del Cauca se compromete a mejorar continuamente la conveniencia, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información (SGSI). Esto se logrará mediante el uso de la política

de seguridad de la información, la gestión de riesgos, los resultados de las auditorías, las acciones correctivas y preventivas y la revisión por la dirección.

Las no conformidades identificadas durante las auditorías y revisiones serán investigadas para determinar sus causas y se tomarán acciones para corregirlas y prevenir su recurrencia. Todas las acciones de mejora serán apropiadas a la magnitud de los problemas e impactos encontrados.

La Universidad asegurará que estas acciones de mejora se implementen y se revise su eficacia, incorporando los aprendizajes en la actualización y fortalecimiento continuo del SGSI.

11. Anexos

1) Instrumento de evaluación MSPI.xlsx
2) Informe de diagnóstico – Enero 2024.pdf
3) Anexo 1 – Matrices del SGSI.xlsx
4) Anexo 2 – Roles y responsabilidades en seguridad de la información.pdf
5) Plan de tratamiento de riesgos de seguridad y privacidad de la información.pdf
6) Procedimiento de Identificación, clasificación y protección de activos tecnológicos críticos.pdf
7) Resumen ejecutivo – SGSI.pdf
8) Manual de políticas de seguridad y privacidad de la información.pdf