PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
_____	_____	_____
Director Gestión de Recursos Tecnológicos - Contratista Seguridad de la Información	Director Gestión de Recursos Tecnológicos	Rector(a)

CONTENIDO

1. INTRODUCCIÓN

La Institución Universitaria Colegio Mayor del Cauca, consciente de la importancia de asegurar la información, debe generar un marco normativo soportado en los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) emitido por MINTIC, el componente transversal de la estrategia Gobierno Digital y la norma ISO/IEC 27001:2022 garantizando la Confidencialidad, Integridad y Disponibilidad de la información coadyuvando al cumplimiento de la misión y los objetivos institucionales. El Plan de Seguridad y Privacidad de la Información (PSPI), está encaminado al fortalecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) de la Institución Universitaria Colegio Mayor del Cauca; conformado por políticas, procedimientos, responsabilidades y controles generados para minimizar riesgos relacionados con la información.

2. JUSTIFICACIÓN

Para garantizar la confidencialidad, Integridad y Disponibilidad de la información en la Institución Universitaria Colegio Mayor del Cauca el proceso Gestión de Recursos Tecnológicos genera el Plan de Seguridad y Privacidad de la Información tomando como referencia las directrices del Modelo de Seguridad y Privacidad de la Información emitido por MINTIC, recomendaciones técnicas de la norma ISO/IEC 27001 del 2022, requerimientos de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, las cuales se deben tener en cuenta para la gestión de la información; permitiendo de esta manera la construcción de un estado más participativo, transparente y eficiente.

3. ALCANCE

El plan de seguridad y privacidad de la información (PSPI) aplica para todos los procesos de la institución Universitaria Colegio Mayor del Cauca los cuales manejen, procesen o interactúen con información física y/o digital

4. OBJETIVO

4.1 GENERAL

Generar El Plan de Seguridad y Privacidad de la Información (PSPI) para la Institución Universitaria Colegio Mayor del Cauca, basado en los requisitos de Gobierno Digital y la norma ISO/IEC 27001:2022 garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

4.2 ESPECÍFICOS

- Generar lineamientos de seguridad y privacidad de la información tomando como referencia el SGSI (Sistema de Gestión de Seguridad de la Información) de la Institución Universitaria Colegio Mayor del Cauca IUCMC y los requerimientos del MSPI (Modelo de Seguridad y Privacidad de la Información).
- Promover el uso de mejores prácticas de seguridad y privacidad de la información en los procesos Institucionales.
- Contribuir en la gestión de riesgos relacionados con seguridad de la información.

5. TÉRMINOS Y DEFINICIONES

Activo De Información: Conocimiento o información que tiene valor para la organización.

Activo: Cualquier cosa que tenga valor para la organización. [ISO 27001:2022]

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis De Riesgo: Estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir. (ISO/IEC 27000).

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

CID: Trilogía de seguridad de la información, conformado por los pilares Confidencialidad, Integridad y Disponibilidad.

Confidencialidad: Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000: 2022].

Continuidad Del Negocio: Capacidad de la organización para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial. [22301: 2022].

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. [ISO 27001:2022]

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [ISO/IEC 27000: 2022]

Información Digital: Es toda aquella información que es almacenada o transmitida empleando unos y ceros (el sistema binario). Estos unos y ceros representan un estado real de materia, onda o energía. Por ejemplo, en un disco óptico (CD, DVD…) [http://www.alegsa.com.ar/Dic/informacion_digital.php]

Información: Conjunto organizado y con sentido de datos.

Integridad: Propiedad de exactitud y completitud. [ISO/IEC 27000: 2022].

MSPI: Modelo de Seguridad y Privacidad de la Información emitido por MINTIC

NIST: Instituto Nacional de Estándares y Tecnologías por sus siglas en Ingles de National Institute of Standards and Technology.

No repudio: Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Política: Intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000: 2022].

PSPI: Plan de Seguridad y Privacidad de la Información

Relay: El relay funciona como un interruptor, permitiendo o negando el paso de la corriente eléctrica

Riesgo: Representa la posibilidad o probabilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos. (Administración del Riesgo - 1.0.P.04 – SAIC Colegio Mayor del Cauca).

SAIC: Sistema de Aseguramiento Interno de la Calidad [Institución Universitaria colegio Mayor del Cauca]

Segregación: Reparto de tareas sensibles entre distintos empleados y/o activos para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia. (ISO27000)

Seguridad De La Información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas. [ISO/IEC 27000: 2022].

SGSI: Sistema De Gestión De La Seguridad De La Información; interrelación de elementos que utiliza una organización donde se determinan políticas, objetivos y controles de Seguridad de la Información con, basado en un enfoque de gestión del riesgo y de mejora continua.

Vulnerabilidad: Una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN[1]

La Institución Universitaria Colegio Mayor del Cauca adopta el modelo de seguridad y privacidad de la información de la Estrategia de Gobierno Digital que contempla 5 fases, permitiendo el aseguramiento de la información a través de políticas, procedimientos, controles, análisis de riesgos, roles, responsabilidades y buenas prácticas.

El modelo contempla 6 niveles de madurez, donde claramente se puede identificar la evolución en la implementación del modelo.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno Digital, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

[1] Modelo de Seguridad y Privacidad de la Información _ MINTIC.
https://gobiernodigital.mintic.gov.co/692/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Figura 1. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información (MSPI)

6.1 FASE DE DIAGNÓSTICO DEL MSPI

Fase para determinar el estado actual de la Institución Universitaria Colegio Mayor del Cauca basado en los requerimientos del MSPI-MINTIC

Figura 2. Fase de Diagnostico

DIAGNOSTICO			
METAS	Actividades/Instrumentos	TIEMPO ESTIMADO	RESULTADOS
Determinar el estado actual de la gestión de seguridad y privacidad de la información al	Diligenciamiento del Instrumento Evaluación MSPI emitido por MINTIC.	19/01/2025 - 18/12/2025	Instrumento Evaluación MSPI con la valoración del

interior de la Institución Universitaria			estado actual de la gestión de seguridad y privacidad de la información.
Identificar el nivel de madurez de seguridad y privacidad de la Información de la Institución Universitaria	Valoración del nivel de madurez disponible en el documento: "Modelo de Seguridad y Privacidad de la Información (MSPI)" estrategia Gobierno Digital.		
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planeación.	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Institución Universitaria Colegio Mayor del Cauca.	19/01/2025 - 18/12/2025	Declaración de Aplicabilidad. Riesgos actualizados

Para desarrollar la fase de diagnóstico la Institución Universitaria Colegio Mayor del Cauca debe realizar la recolección de información haciendo uso de la herramienta MSPI (Modelo de Seguridad y Privacidad de la Información) de diagnóstico emitida por el Ministerio de las TIC (MINTIC).

6.1.1 ESTADO ACTUAL DE LA ENTIDAD

El resultado obtenido del diagnóstico inicial permite conocer la manera como se ejecutan las actividades y a partir de ahí poder planear de la mejor manera el Sistema de Seguridad y Privacidad de la Información.

EFECTIVIDAD DE CONTROLES

La Institución Universitaria obtuvo una calificación de 77 sobre 100, clasificándonos en el nivel GESTIONADO, es decir que se evidencia que, 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.

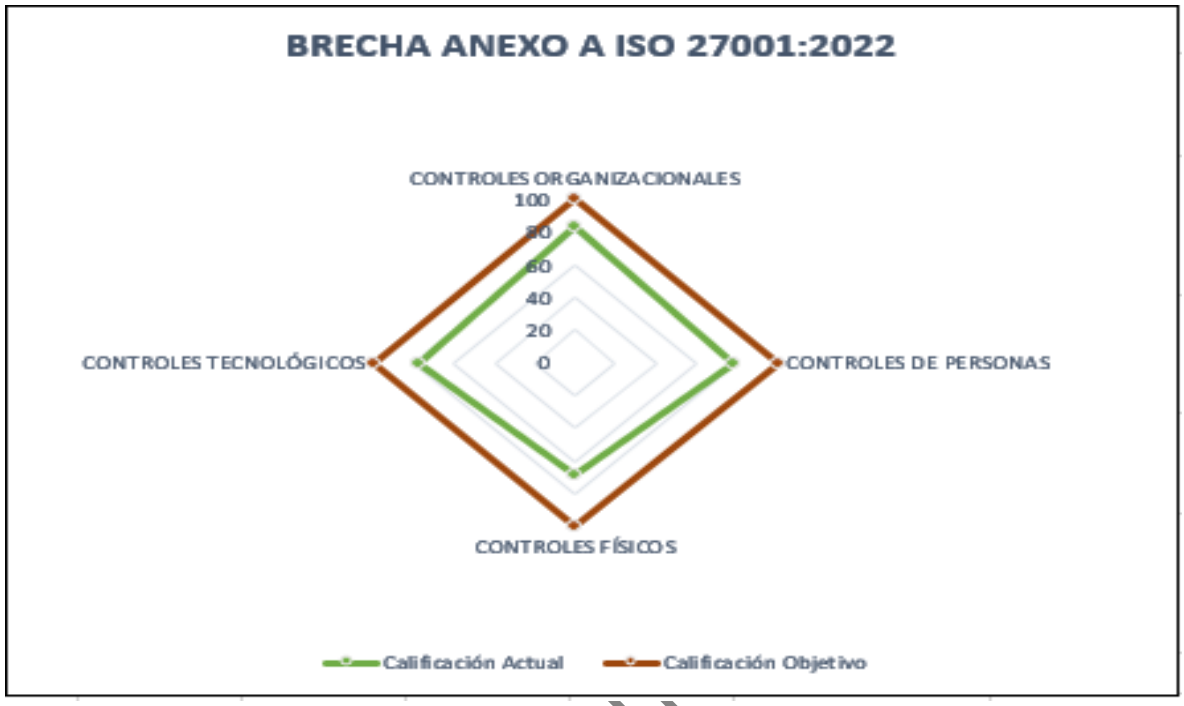
No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	83	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	78	100	GESTIONADO
A.7	CONTROLES FÍSICOS	69	100	GESTIONADO
A.8	CONTROLES TECNOLÓGICOS	77	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		77	100	GESTIONADO

Se deben MEJORAR los controles A.7. controles físicos ya que obtuvieron una calificación BUENA que oscila entre 70-71 puntos, los demás controles se deben MANTENER Y MEJORAR en el tiempo debido a que obtuvieron una calificación elevada de acuerdo con la norma ISO 27001:2022 en su anexo A.

6.1.2 BRECHA ANEXO A - ISO 27001:2022

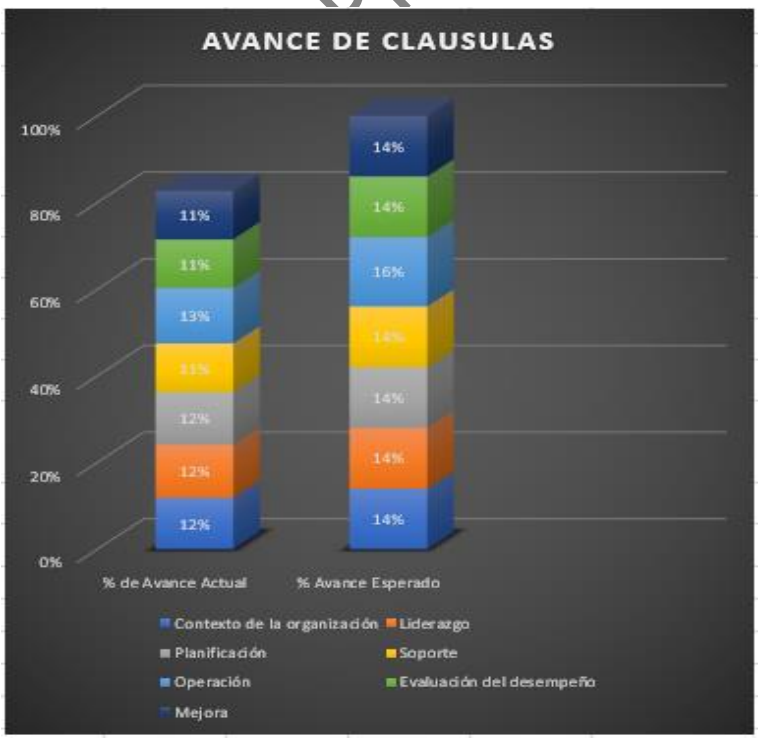
La siguiente gráfica muestra que la Institución Universitaria está en proceso GESTIONADO frente a la implementación de controles relacionados con Seguridad y privacidad de la Información (norma ISO 27001:2022), los activos que la contienen y los medios relacionados.

La brecha encontrada, se puede apreciar en la siguiente gráfica, evidenciando el riesgo al que se encuentra expuesta la información.



CICLO PHVA

Otro de los aspectos evaluados dentro de la herramienta MSPI suministrada por MINTIC es el ciclo PHVA, el cual está alineado con los plazos anuales dados para el cumplimiento de Gobierno en Línea (Hoy Gobierno Digital).



Los resultados obtenidos del cumplimiento de la norma ISO/IEC: 27001:2022 se representan de manera general en el siguiente grafico

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	12%	14%
		Liderazgo	12%	14%
		Planificación	12%	14%
		Soporte	11%	14%
	Implementación	Operación	13%	16%
	Evaluación de Desempeño	Evaluación del desempeño	11%	14%
	Mejora Continua	Mejora	11%	14%
TOTAL			83%	100%

6.2 FASE DE PLANEACIÓN

Para desarrollar esta fase, la Institución Universitaria toma como punto de partida los resultados obtenidos en la fase anterior, generar el plan de Seguridad y privacidad de la información involucrando las políticas y lineamientos establecidos dentro del SAIC (Sistema de Aseguramiento Interno de la Calidad) y el plan de tratamiento de riesgos de seguridad y privacidad de la información.

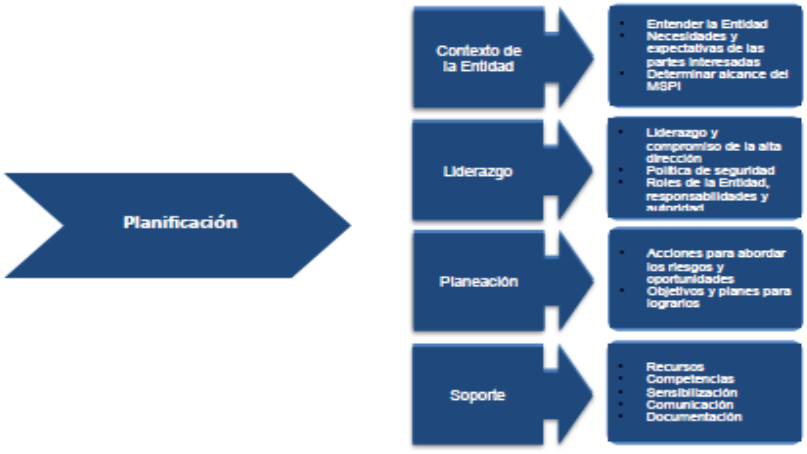


Figura 3. Fase de planificación[2]

6.2.1 PLAN DE SEGURIDAD DE LA INFORMACIÓN

PLANEACIÓN			
METAS	Actividades/Instrumentos	TIEMPO ESTIMADO	RESULTADOS
Política de seguridad y privacidad de la información.	Actualizar la política de seguridad y privacidad de la información.	19/01/2025 - 19/06/2025	Política de seguridad y privacidad de la información.
	Revisión y actualización de procedimientos de seguridad y privacidad de la información.		Procedimientos, manuales y/o formatos de seguridad y privacidad de la información debidamente socializados y aprobados por el comité de seguridad y privacidad de la información.
Roles y responsabilidades del comité de seguridad y privacidad de la información.	Revisión y actualización del documento roles y responsabilidades del comité de seguridad (o quien haga sus veces)	19/01/2025 - 19/06/2025	Documento roles y responsabilidades del comité se seguridad y privacidad aprobado y publicado en SAIC.
Inventario activo de información y gestión de riesgos.	Actualización inventario activos de información de acuerdo al plan de tratamiento de riesgo.	19/01/2025 - 19/06/2025	Documentos activos de información actualizada. Actualización y gestión de riesgos en aplicativo Institucional.
Plan de comunicaciones de seguridad de la información.	Revisar, solicitar y actualizar documentos en página web	19/01/2025 - 19/06/2025	Documentos o procedimientos actualizados

6.2.2 POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Institución Universitaria Colegio Mayor del Cauca, entiende y conoce la existencia de riesgos en seguridad de la información que pueden afectar el desarrollo de la misión institucional. Por

[2] Tomado de la guía "Modelo de Seguridad y Privacidad de la Información – MINTIC"

ello, se compromete a realizar las tareas necesarias para mantener la confidencialidad, integridad y disponibilidad de los activos de la información, mediante una gestión de riesgos, asignación de responsabilidades en seguridad y la participación activa de las partes interesadas, cumpliendo con la normatividad vigente y para lograr la mejora continua.

6.2.3 OBJETIVOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- ✓ Proteger los activos de la información en términos de su confidencialidad, integridad y disponibilidad que permiten la prestación de los servicios de la Institución Universitaria Colegio Mayor del Cauca.
- ✓ Atender y solucionar los incidentes de seguridad de la información reportados en la Institución Universitaria.
- ✓ Sensibilizar al personal de la Institución en seguridad de la información, buscando el compromiso en el cumplimiento de políticas de seguridad de la información, reporte de incidentes de seguridad a través de los canales autorizados y participación periódica en la gestión de riesgos.

6.2.4 ROLES Y RESPONSABILIDADES

El documento 1.04.30.103.D.11 Roles Y Responsabilidades Seguridad De La Información, disponible en el link https://campus2.unimayor.edu.co/CampusSGI https://campus2.unimayor.edu.co/CampusSGI/ opción: Campus Unimayor SAIC/Gestión de Recursos Tecnológicos/Seguridad de la Información/Documentos, lista tanto las responsabilidades como los integrantes del Comité del Sistema de Gestión de Seguridad de la Información.

Participantes del comité:

- ✓ Rector
- ✓ Responsable de Seguridad de la Información
- ✓ Director Gestión de Recursos Tecnológicos
- ✓ Profesional Universitario de Calidad
- ✓ Profesional Universitario de Gestión Documental

6.2.5 INVENTARIO ACTIVOS DE INFORMACIÓN

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
[S] SERVICIOS				
1.	[S_ACADEMICO_ADMINISTRATIVO] Servicios CAMPUS	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	NA

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
2.	[S_WEB]	Gestión de Comunicaciones y Gestión de Recursos Tecnológicos	Web master P.U. Comunicaciones Contratista Externo	
3.	[S_WIFI]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
4.	[S_CORREO_ELECTRONICO]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
5.	[S_TELFONIA_IP]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
6.	[S_DHCP]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
7.	[S_MAQUINAS_V]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
8.	[S_ANTIVIRUS]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
9.	[S_CAMARAS_IP]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
10	[S_FINANCIERO]	Gestión Financiera y Contable	Director Gestión Financiera y Contable	
11	[S_CATALOGO_BIBLIOTECA]	Gestión de Biblioteca	PU Biblioteca	
12	[S_MOODLE]	Gestión Recursos Tecnológicos	Director Unimayor Virtual	
13	[S_DNS]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
14	[S_BACKUPS]	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
15	[S_Inventario_Incidencias]	Gestión Recursos Tecnológicos	Director de Gestión Recursos Tecnológicos	
16	[INFO_R] Información restringida	Gestión Documental	P.U. Gestión Documental	
17	[INFO_PUBLICA]	Gestión Documental	P.U. Gestión Documental	
18	[S_VoIP] Sistema de Telefonía IP Nube	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
[S] APLICACIONES (Software)				

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
19	[S_CAMPUS_A] Campus Académico	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Decanos, Coordinadores de programa, secretarios académicos y Auxiliares administrativas de las facultades de la institución.
20	[S_CAMPUS_AE] Campus Académico Extensión	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Decanos, Coordinadores de programa, secretarios académicos y Auxiliares administrativas
21	[S_CAMPUS_AEG] Módulo Administrador Egresados	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo encargado de la oficina de egresado.
22	[S_CAMPUS_AD] Módulo ADMISIONES	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo, asesor y auxiliares encargados de la oficina de admisiones.
23	[S_CAMPUS_BO] Módulo Banco De Oferentes)	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal Docente
24	[S_CAMPUS_B] Módulo Bienestar	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo asesor, contratistas psicología de Desarrollo Humano de bienestar institucional
25	[S_CAMPUS_CN] Módulo Consulta de Notas	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Estudiantes de la Institución Unimayor.
26	[S_CAMPUS_CF] Módulo Consulta Financiera	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo del

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
				Proceso Gestión Financiera y Contable
27	[S_CAMPUS_C] Módulo Contratación	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal líderes de proceso, Decano, secretario académico, coordinador académico
28	[S_CAMPUS_I] Módulo Internacionalización	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo de la oficina de internacionalización
29	[S_CAMPUS_IN] Módulo INVESTIGACIONES	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo del área de investigaciones.
30	[S_CAMPUS_LD] Módulo Labor Docente	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal líderes del proceso, Decanos, secretario académico, vicerrectoría, rectoría y talento humano.
31	[S_CAMPUS_LR Módulo LIQUIDACIÓN RECAUDOS]	Gestión Recursos Tecnológicos	P.U. Sistemas de Información. Director Admisiones.	Auxiliares administrativos de las facultades y personal de la oficina de financiera de la institución.
32	[S_CAMPUS_P] Módulo Planeación	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo Líderes de procesos de la institución decanos secretario vicerrector coordinador y

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
				personal de la oficina de planeación.
33	[S_CAMPUS_RN] Módulo Registro Notas	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Docentes de la Institución Unimayor.
34	[S_CAMPUS_R] Módulo Reportes	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo, Rectoría, Vicerrectoría, Decanos, coordinadores académicos, secretarios académicos, auxiliares de la facultad, bienestar y oficina de autoevaluación SAIC.
35	[S_CAMPUS_SAIC] Módulo SAIC (Sistema de Aseguramiento Interno de la Calidad)	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Todo el personal de la Institución Unimayor.
36	[S_CAMPUS_E] Módulo Encuestas	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Funcionarios, contratistas, administrativos de la institución.
37	[S_CAMPUS_PE] Módulo Panel Evaluador	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Docentes internos y externos de la institución que hayan sido asignados por los coordinadores de programa.
38	[S_ CAMPUS_TM] Módulo Task Manager	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Administrativos sistemas de información y TIC.
39	[S_CAMPUS_D] Módulo Desarrollo	Gestión Recursos Tecnológicos	P.U. Sistemas de Información.	Administrativos de la oficina de sistemas de información.
40	[S_CAMPUS_AC] Módulo Acreditación		P.U. Sistemas de Información.	Administrativos de acreditación

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
41	[S_CAMPUS_CI] Módulo Control Interno	Gestión Recursos Tecnológicos	P.U. Sistemas de Información.	Administrativo de control interno
42	[S_ CAMPUS_EG] Módulo Egresados	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Egresados de la Institución Unimayor.
43	[S_CAMPUS_FA] Módulo Factura Admitidos	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Aspirantes de la institución
44	[S_CAMPUS_FI] Módulo Factura Inscripción	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Aspirantes de la institución
45	[S_CAMPUS_F] Módulo Funcionarios	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Personal administrativo de la Institución Unimayor.
46	[S_CAMPUS_P] Módulo Permanencia	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Administrativos socioeconómico y Líder del proceso de bienestar.
47	[S_CAMPUS_PR] Módulo Préstamo de Recursos	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Administrativo y líder de las TIC.
48	[S_CAMPUS_PS] Módulo Proyección Social	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Coordinadores de las facultades y Personal administrativo de la oficina de proyección social
49	[S_CAMPUS_RF] Módulo Recursos Físicos	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Pasante y administrativo y líder de las TIC.
50	[S_CAMPUS_RELMI] Módulo Registro en Línea Matrícula Programa de Extensión Ingles	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Decanos, Coordinadores de programa, secretarios académicos y Auxiliares administrativas de las facultades de la institución.
51	[S_CAMPUS_RC] Módulo Registro Cultura	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Estudiantes, egresados, funcionarios y administrativos de la institución.

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
52.	[S_CAMPUS_REL] Módulo Registro en Línea	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Aspirantes que ya cuentan con un PIN para el respectivo registro en línea.
53.	[S_CAMPUS_RS] Módulo Registro Seminario	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Decanos, Coordinadores de programa, secretarios académicos y Auxiliares administrativas y de las facultades de la institución. Asistentes a los eventos realizados por la institución
54.	[S_CAMPUS_RE] Módulo Restore	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Auxiliares administrativas de cada facultad, estudiantes, egresados, funcionarios y Docentes.
55.	[S_CAMPUS_SE] Módulo Sistema Electoral	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Líder y Auxiliares administrativas de Secretaría General.
56.	[S_CAMPUS_TH] Módulo Talento Humano	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Líder y Auxiliares administrativas de talento humano.
57.	[S_CAMPUS_CIF] Módulo Cifrador	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Líder y contratistas de la oficina sistema de información.
58.	[S_CAMPUS_DE] Módulo Registro Deportes	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Todo el personal de la Institución Unimayor.
59.	[S_CAMPUS_PSE] Módulo PSE	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Aspirantes, estudiantes, egresados, docentes, funcionarios, contratistas, administrativos y todo personal de la institución.
60.	[S_CAMPUS_AL] Módulo Almacén	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Almacenista general

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
61	[S_CAMPUS_CL] Módulo Conexión Laboral	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Egresados, responsable de egresados, representante legal de empresas registradas
62	[S_CAMPUS_SG] Módulo Secretaría General	Gestión Recursos Tecnológicos	P.U. Sistemas de Información	Auxiliares administrativas de Secretaría General
63	[S_HELPDESK] Sistema Inventario e Incidencias de Activos de TI	Gestión Recursos Tecnológicos	Director de Gestión de Recursos Tecnológicos	Super_administrador Administrador Técnico Post_Only
64	[S_Directorio] Sistema Web Directorio Institucional	Gestión Recursos Tecnológicos	Director de Gestión de Recursos Tecnológicos	Oficina TIC y comunicaciones. Permisos:
65	[S_RESERVAS] Sistema de Reservas de Salas de Reunión	Gestión Recursos Tecnológicos	Director de Gestión de Recursos Tecnológicos Contratista TIC	Administrador Usuario Normal
66	[S_ENC] Sistema de Encuestas Unimayor	Gestión Recursos Tecnológicos	Director de Gestión de Recursos Tecnológicos Contratista TIC	Administrador
67	[S_CELESTE] Sistema Contable y Financiero	Dirección Financiera y Contable	Director(a) Financiero(a) y Contable	Administrador Usuario funcional
68	[S_CATALOGO_BIBLIOTECA] Sistema Integrado de Gestión de Bibliotecas	Gestión de Biblioteca	Bibliotecólogo	Usuario
69	[S_PQRS] Sistema de PQRS (ORFEO)	Gestión Recursos Tecnológicos	Director de Gestión de Recursos Tecnológicos Contratista TIC	Administrador Usuario Normal
[HW] EQUIPOS INFORMÁTICOS (Servidores, Hardware)				
70	[SER_BCP_CAMPUS] Servidor Business Continuity Plan del Campus	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
71	[SER_CAMPUS] Servidor Sistema de Información Académica y Gestión	Gestión Recursos Tecnológicos	P.U Seguridad Digital	Personal administrativo con acceso a los diferentes módulos del CAMPUS

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
72	[SER_WEB_BACKUPS] Servidor sitios Web	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
73	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
74	[SER_PRUEBAS_CAMPUS] Servidor Pruebas Campus	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
75	[SER_PANTALLAS] Servidor Pantallas Informativas y Aplicaciones WEB	Gestión Recursos tecnológicos	P.U Seguridad Digital	
76	[SER_SNIES] Servidor SNIES	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
77	[SER_CELESTE] Servidor Sistema Financiero y Contable	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
78	[SER_CATALOGO_BIBLIOTECA] Servidor Catálogo Biblioteca	Gestión de Biblioteca	PU Biblioteca	
79	[SER_MOODLE_DNS] Servidor Herramientas Virtuales de Aprendizaje	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
80	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
81	[HW_PC] Equipos de cómputo (escritorio y portátiles)	Todos	Todos	
82	[HW_IMP] Impresoras	Administrativos - Docentes	Todos	
83	[HW_ESC] Escáneres	Administrativos - Docentes	Todos	
84	[HW_SWIT] Switchs administrable	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
85	[HW_FW] Firewall UTM	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
86	[HW_WAP] Puntos de Acceso Inalámbrico	Gestión Recursos Tecnológicos	P.U Seguridad Digital	
87	[HW_enrutadores] Enrutadores	Gestión Recursos Tecnológicos	Proveedor ISP	
88	[HW_Radio_Enlace] Radio Enlace Interconexión Alterna	Gestión Recursos Tecnológicos	P.U Seguridad Digital	

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
89	[HW_Gateway] Gateway VoIP	Gestión Recursos Tecnológicos	Proveedor ISP	
[COM] Redes de Comunicaciones				
90	[COM_RT] Red Telefónica	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
91	[COM_Datos] Red de Datos	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
92	[COM_WIFI] Red inalámbrica	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
93	[COM_MAN] Red Área Metropolitana	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
94	[COM_ISP] Internet	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
[SI] SOPORTES INFORMACIÓN				
95	[SI_USB] Soportes de información en Discos Externos USB	Todos	Todos	
96	[SI_IMPRESOS] Soportes de Información Impresos en Papel	Todos	Todos	
97	[SI_NAS] Almacenamiento en la Red	Gestión Recursos Tecnológicos	Todos	
98	[SI_AA] Almacenamiento de archivos en nube Privada	Gestión Recursos Tecnológicos	Todos	
99	[SI_Drive] Almacenamiento en la Nube (Gmail)	Todos	Todos	
10	[SI_OCI] Almacenamiento en Oracle Cloud Infrastructure	Gestión Recursos Tecnológicos	Todos	
[AUX] EQUIPAMIENTO AUXILIAR				
10	[AUX_UPS] Sistema de Alimentación Ininterrumpida	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
10	[AUX_AC]Aires Acondicionados	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
10	[AUX_Cabl_Elect] Cableado Eléctrico	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
10	[AUX_Cabl_Datos] Cableado Datos	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
10	[AUX_DEST] Equipo Destrucción de Papel	Gestión Documental	P.U. Gestión Documental	
10	[AUX_Tel] Teléfonos	Gestión Recursos Tecnológicos	Todos	
10	[AUX_VIG] Cámaras de Vigilancia	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
10	[AUX_DATAFONO] Datafono	Dirección Financiera y Contable	Tesorero General	
[L] INSTALACIONES				
10	[L_Edificio] Edificios			
11	[L_DATOS] Centros de Datos	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
11	[L_CANAL]Canalización (Cableados)	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
11	[L_GAB] Gabinete de red	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos	
[P] PERSONAL				
11	[P_UE] Usuarios Externos	Gestión de la Información y la Comunicación	P.U. Gestión Documental	
11	[P_UI] Usuarios Internos	Gestión de la Información y la Comunicación	P.U. Gestión Documental	
11	[P_ADM] Administradores de Sistemas	Gestión Recursos Tecnológicos	P.U Sistemas de Información Contratistas TIC	
11	[P_DBA] Administrador de Bases de Datos	Gestión Recursos Tecnológicos	P.U Sistemas de Información Contratistas TIC	
11	[P_SEC] Administradores de seguridad	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos P.U. Seguridad Digital	

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SAIC)	Responsable	Perfiles Usuario
			Contratistas TIC	
11	[P_DES] Desarrollo Software	Gestión Recursos Tecnológicos	P.U Sistemas de Información Contratistas TIC	
11	[P_CON] Contratistas	Gestión Jurídica	Secretario General	
12	[Proveedores] Proveedores	Gestión Jurídica	Secretario General	
12	[P_OCA] Ocasionales	Talento Humano	P.U. Talento Humano	

6.2.6 INTEGRACIÓN MSPI CON EL SISTEMA DE GESTIÓN DOCUMENTAL

De acuerdo al diagnóstico arrojado con el Instrumento MSPI se debe realizar la actualización de activos de información y la actualización de tablas de retención documental formalizando los documentos de seguridad y privacidad de la información.

6.2.7 IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGO

El proceso de identificación, valoración y tratamiento de riesgos se encuentra detallado en el documento 1.04.30.103.D.13 Plan de Tratamiento de Riesgos de seguridad y privacidad de la información disponible en:

https://unimayor.edu.co/web/transparencia/18-unimayor/planeacion/2856-plan-de-tratamiento-de-riesgos-de-seguridad-y-privacidad-de-la-informacion; el cual se debe actualizar cada año.

6.2.8 PLAN DE COMUNICACIONES

La IUCMC, debe incluir dentro del plan de comunicaciones PETI la estrategia de comunicación, sensibilización y capacitación de seguridad y privacidad de la información descrita en el documento 1.04.30.103.D.12 Plan de sensibilización seguridad de la información, disponible en: https://campus2.unimayor.edu.co/CampusSGI/ opción: Campus Unimayor SAIC/Gestión de Recursos Tecnológicos/Seguridad de la Información/Documentos; aplicable en todos los niveles de la entidad (Directivos, funcionarios, academia y terceros)

6.3 FASE DE IMPLEMENTACIÓN

La IUCMC debe desarrollar la planificación realizada en la fase anterior teniendo en cuenta los aspectos más relevantes con el fin de cerrar brechas encontradas en el diagnóstico; en esta fase deberán realizarse las siguientes actividades:

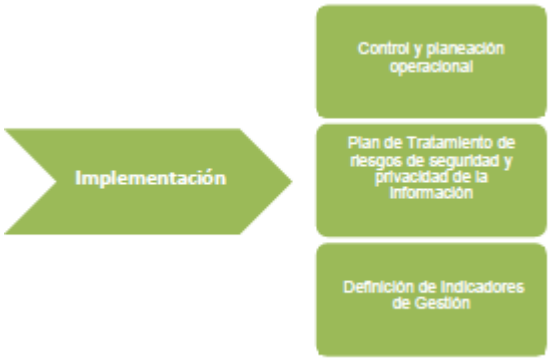


Figura 4. Fase de implementación

6.3.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La IUCMC debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos 2023, las acciones (controles) deben estar registradas según los formatos existentes en el Campus Planeación o aplicativo destinado para tal fin, de igual manera deberá acoger lo estipulado en el procedimiento 1.01.28.80.P.01 Control de documentos.

6.3.2 IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO

Los líderes de proceso deben tomar como hoja de ruta el documento plan de tratamiento de riesgos de seguridad de la información para identificar y aplicar en control adecuado para llevar a un nivel aceptable la entidad, este proceso debe realizarse con el responsable de seguridad y privacidad de la información o el responsable de las TIC.

6.3.3 INDICADORES DE GESTIÓN

Definir y validar por la alta dirección de indicadores que permitan medir:

- ✓ Efectividad en los controles.
- ✓ Eficiencia del MSPI al interior de la entidad.
- ✓ Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- ✓ Comunicar valores de seguridad al interior de la entidad.
- ✓ Servir como insumo al plan de control operacional.

La Institución Universitaria ha generado los indicadores de gestión de seguridad y privacidad de la información en el documento Formulación y control de indicadores de seguridad de la información, siguiendo la guía N°. 9 (Indicadores de gestión de seguridad y privacidad de la información) de MINTIC.

Proceso	Nombre	Objetivo del indicador	Fórmula	Meta	Periodicidad de medición	Responsable de cumplir la meta
Gestión recursos tecnológicos	Incidentes de seguridad de la información (físicos, lógicos, electrónicos)	Monitorear y Reducir el número de incidentes de seguridad de la información	(#Incidentes de seguridad de la información atendidos efectiva y oportunamente/ #total de incidentes reportados) *100	80%	Trimestral	Líder de Seguridad de la información
Gestión y Desarrollo del Talento Humano	Usuarios activos e inactivos	Mantener actualizado los usuarios de los sistemas de información	(# usuarios vigentes o activos en el directorio activo / (Total de personas vigentes en talento humano) * 100	100%	Semestral	P.U. Talento Humano – PU Sistemas de Información – TA Redes
Gestión recursos tecnológicos	Backups y respaldo de infraestructura tecnológica (Hardware – Software, BD y comunicaciones)	Proteger la información de propiedad de IUCMC o de terceros bajo su custodia	(# de Backups realizados / # Total de Backups programados) * 100	100%	Trimestral	Director Gestión de Recursos Tecnológicos
Gestión y Desarrollo del Talento Humano	Protección de la confidencialidad de la información a nivel contractual	Cumplimiento con la aceptación del acuerdo de confidencialidad	(# de empleados y contratistas con acuerdo de confidencialidad firmados / Total de colaboradores) *100	100%	Semestral	P.U. Talento Humano

6.4 FASE DE EVALUACIÓN DE DESEMPEÑO

Terminadas las actividades en la fase de implementación se hace el seguimiento y monitoreo del plan de seguridad y privacidad de la información, para medir la efectividad de los controles a través de los indicadores, se espera que cubra los requisitos del MSPI, Ley de Transparencia y Acceso a la Información Pública.

Las etapas a realizar se resumen en la siguiente gráfica:

Figura 5. Fase de Evaluación y Desempeño

6.4.1 PLAN DE REVISIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DE MSPI

La IUCMC debe generar un plan de revisión y seguimiento que contemple las siguientes actividades:

ACTIVIDAD	PERIODICIDAD DE EJECUCIÓN
Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.	Anual
Seguimiento a la programación y ejecución de las actividades de auditorías internas y externas del MSPI.	Anual
Seguimiento al alcance y a la implementación del MSPI.	Anual
Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.	Anual
Revisión de indicadores de gestión de seguridad de la información.	Anual
Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI).	Una vez al año

6.4.2 PLAN DE EJECUCIÓN DE AUDITORIAS

La IUCMC realizará las auditorias siguiendo lo dispuesto en el documento 1.02.P.03 AUDITORÍAS, disponible en consulta documentos: https://campus2.unimayor.edu.co/CampusSGIA/buscador/AUDITOR%C3%8DAS, debe adicionar dentro del plan de auditorías la revisión del Sistema de Gestión de Seguridad y Privacidad de la información y los controles implementados a través del MSPI.

6.5 FASE DE MEJORA CONTINUA

La IUCMC debe consolidar los resultados obtenidos en la fase anterior "Evaluación y desempeño" y realizar los correctivos necesarios para mitigar las debilidades encontradas.

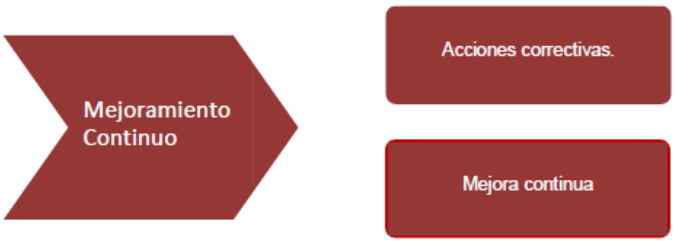


Figura 6. Fase de Mejora Continua

Las acciones de mejora (acciones preventivas, correctivas y/o de mejora) resultado de auditorías y/o seguimientos internos, son tratadas de acuerdo con el Proceso de planeación y Mejora Continúa tomando como referencia el procedimiento 1.01.28.80.P.03 PLANES DE MEJORAMIENTO(https://campus2.unimayor.edu.co/CampusSGIA/buscador/PLANES%20DE%20MEJORAMIENTO)

7. MODELO DE MADUREZ

El nivel de madurez en la Institución Universitaria Colegio Mayor del Cauca referente a seguridad y privacidad de la información se identifica valorando el cumplimiento de controles administrativos y técnicos haciendo uso del Instrumento de diagnóstico del MSPI emitido por MINTIC.

Después de evaluar el nivel de cumplimiento de los 93 controles agrupados en los 4 temas (organizacionales, de personas, físicos y tecnológicos) definidos en el Anexo A de la norma ISO/IEC 27001:2022, así como los lineamientos y buenas prácticas del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), se obtuvo una calificación global del 79 %, lo cual permite clasificar el nivel de madurez del sistema de gestión de la seguridad de la información como "Gestionado", conforme se detalla en la siguiente gráfica.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	83	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	78	100	GESTIONADO
A.7	CONTROLES FÍSICOS	69	100	GESTIONADO
A.8	CONTROLES TECNOLÓGICOS	77	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		77	100	GESTIONADO

8. ADOPCIÓN DEL PROTOCOLO IPV6

8.1 FASE DE PLANEACIÓN

Entre el año 2015 y 2016 se documentó una mejora institucional (Número 87) encaminada a Implementar la transición del protocolo IPV4 a IPV6, basado en la metodología dual-stack la cual permite implementar el protocolo Ipv6 y la mantener el protocolo Ipv4, con el fin de garantizar que los servicios de red relevantes funcionen en esta modalidad y de forma segura.

En el año 2018 se realizó un trabajo de grado de la Facultad Ingeniería cuyo objetivo fue levantar el diagnóstico del nivel de implementación y prácticas encaminadas a verificar el funcionamiento de Ipv6 e Ipv4 en al menos un servicio de red en la Institución.

Para julio del año 2019 realizó la actualización de Ipv6 en todo el direccionamiento de red, incluido red Wifi; activando una funcionalidad en el UTM que sirva de relay para enviar el direccionamiento a las diferentes subredes paralelo activar las funcionalidades necesarias en el UTM para el análisis de tráfico y aplicación de los módulos de protección.

En el año 2025 se realizó la actividad denominada "DOCUMENTAR EL PLAN DE CONTINGENCIA PARA IPV6." En este documento se ingresaron las diferentes actividades realizadas en el IV Trimestre de 2025, dentro de las cuales se encuentran:

- Se actualizaron en la Plataforma de seguimiento del MinTIC las etapas correspondientes a la Fase II — Implementación del Protocolo IPv6.
- De igual manera, después de que se realizó la codificación y el ingreso en el Sistema de Información Campus SAIC de los documentos Plan de Contingencia IPv6 y Fase III Pruebas de Funcionalidad IPv6, se hizo la carga de las evidencias dentro de las etapas de la Fase III en la plataforma de seguimiento IPv6.
- Finalmente, se notificó al funcionario del MinTIC, para que posteriormente, se realice la correspondiente revisión y aprobación.

8.2 FASE DE IMPLEMENTACIÓN

La IUCMC cumpliendo con los requerimientos dados por el ministerio de tecnologías de información y comunicación (Min TIC) para la adopción del protocolo Ipv6 al interior de las instituciones públicas en su propia infraestructura.; realizó e implemento el diseño de direccionamiento, con los siguientes rangos:

Administrativos 2001:13f8:1507:1100::2 – 2001:13f8:1507:1100::5ª

Financiera 2001:13f8:1507:1400::2 – 2001:13f8:1507:1400:1e

Inalámbrica 2001:13f8:1507:1300::2 – 2001:13f8:1507:1300:1f4

Salas de Cómputo 2001:13f8:1507:1200::2 – 2001:13f8:1507:1200::78

Servidores 2001:13f8:1507:1f00::2 – 2001:13f8:1507:1f00::28

VoIp 2001:13f8:1507:1500::2 – 2001:13f8:1507:1500::1.

8.3 PRUEBAS DE FUNCIONALIDAD

Se realizó la instalación de un servidor DHCP (de prueba) con capacidades de Ipv6 para las diferentes subredes.

Durante los años 2018 y 2019 se adecuó, actualizó e instaló un servidor DHCP principal dual stack Ipv4-Ipv6 y un servidor de respaldo con la misma configuración; de igual manera se logró

configurar por parte del proveedor de VPS (Virtual Private Server) los servicios DNS y WEB en Ipv6 – Ipv4.

Se actualizaron documentos PLAN DE CONTIGENCIA TRANSICIÓN IPV6, IMPLEMETACIÓN PROTOCOLO IPV6 FASE II, FASE III PRUEBAS DE FUNCIONALIDAD DE IPV6, PLAN DE TRANSICIÓN IPV6 FASE I Y PLAN DE ESTRATEGIA DE TRANSICIÓN DE IPV4 A IPV6.

9. NORMAS

El modelo de Seguridad y privacidad de la información en la institución Universitaria Colegio Mayor del Cauca se basa principalmente en la siguiente normativa:

Ley 1266 de 2008: Por el cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales.

Ley 1341 de 2009: principios y conceptos de la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones.

Ley 1581 de 2012: Protección de datos personales

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la ley de datos personales

Ley 1712 de 2014: Por el cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones y se define el componente de Seguridad y privacidad de la información, como parte de la estrategia Gobierno en Línea (GEL).

10. DOCUMENTOS DE REFERENCIA

Guía # 14. Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información. MINTIC.

Instructivo Seguridad y Privacidad de la Información. MINTIC
Herramienta de Diagnóstico de Seguridad y Privacidad
1.04.30.103.P.07 Procedimiento para Continuidad del Negocio
1.04.30.103.R.20 Formato Declaración de Aplicabilidad
1.04.30.103.P.08 Gestión de Incidentes de Seguridad de la Información
1.0.D.03 Política, alcance y objetivos de seguridad de la información

1.04.30.103.D.11 Roles y Responsabilidades Seguridad de la Información
1.04.30.103.D.12 Plan de Sensibilización Seguridad de la Información
1.01.D.17 Política Control de Acceso de Seguridad de La Información
1.0.D.18 Política Desarrollo Seguro de Seguridad de la Información
1.0.D.19 Política Gestión de los Activos de Información de Seguridad de La Información
1.0.D.20 Política de Seguridad para Proveedores
1.04.30.103.D.19 Plan de Seguridad y Privacidad de la Información
1.04.30.103.D.13 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
1.04.30.103.R.19 Reporte de Incidentes de Seguridad de la Información
1.2.2.P.01 Convocatoria, Selección, Vinculación y Retiro de Personal
1.2.2.30.P.04 Formación y Capacitación del Personal
1.01.28.80.P.03 Acciones Correctivas, Planes de Mejoramiento y Proyectos de mejora
1.01.28.80.P.01 Control De Documentos
1.02.P.03 Auditorías

11. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIO REALIZADO
31/05/2019	Se realizó actualización de documento alineado con los resultados obtenidos del diagnóstico MSPI (Modelo de Seguridad y Privacidad de la Información) emitido por MINTIC (Ministerio de Tecnologías de Información y las Tecnologías), Plan de tratamiento de riesgos Además de adicionar documentos de referencia.
02/12/2019	Se realizó actualización de documento alineado con los resultados obtenidos del diagnóstico MSPI (Modelo de Seguridad y Privacidad de la Información) emitido por MINTIC (Ministerio de Tecnologías de Información y las Tecnologías), Plan de tratamiento de riesgos. Además de adicionar documentos de referencia.
26/01/2021	Se realizó actualización de documento alineado con los resultados obtenidos del diagnóstico MSPI emitido por MINTIC.
27/01/2022	Se realizó actualización de documento alineado con los resultados obtenidos del diagnóstico MSPI emitido por MINTIC.
06/09/2022	Se actualizó código del documento según TRD. Se actualizó denominación del proceso, según nuevo mapa de procesos. Se actualizó denominación de cargos responsables, según nueva estructura

	organizacional. Se actualizó código y nombres de documentos de referencia.
13/10/2022	Se actualiza el Plan de seguridad según revisión realizada por el proceso de Gestión de Recursos Tecnológicos.
26/01/2023	Se actualizan las fechas de diagnóstico y planeación. Se actualiza el término SGI a SAIC. Se verifican y actualizan los enlaces de documentos, páginas web y la codificación documental.
24/01/2024	Se actualizan enlaces de referencia a la documentación presente en el plan de seguridad y privacidad, así como la actualización de algunos activos de información.
9 de abril de 2024	Se actualiza código según TRD aprobadas por el Consejo Departamental de Archivos.
23 de enero de 2025	Se realizó la revisión y actualización de los enlaces de documentos, páginas web, la codificación documental y también de algunos activos de información.
26 de enero de 2026	• Ajuste de la citación de la norma iso 27000:2022 y mspi versión 2025 en general. • Se actualizo la tabla del numeral 6.1.1 con la tabla AVANCE CLÁUSULAS DEL MODELO DE OPERACIÓN (PHVA) del MSPI 2025. • Se realizó el ajuste del numeral 6.1.2 actualizando el anexo de Brecha generada por el MSPI 2025 y el gráfico de medida del ciclo PHVA avance de cláusulas, y la tabla de efectividad de controles. • Se ajustaron las fechas del ítem 6.2.1 de entregables. • Actualización del numeral 6.4.1 en cuanto a definición de periodicidad. • Actualización del numeral 6.2.5 en cuanto al inventario de activos identificados en el Plan de Tratamiento de Riesgos. • Actualización del numeral 6.5 en relación al la ruta y nombre del documento relacionado como Plan de Mejoramiento. • Actualización del numeral 7 en descripción y la tabla de evaluación de controles. • Se actualizó el numeral 8.1 en las fases de planeación. • Se actualizaron los documentos de las fases II y III en la plataforma Adopción de IPv6 - Gobierno digital - MinTIC.