PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

COPIA CONTROLADA

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 4
2. JUSTIFICACIÓN 4
3. ALCANCE 4
4. OBJETIVO 4
4.1 GENERAL 4
4.2 ESPECÍFICOS 5
5. TÉRMINOS Y DEFINICIONES 5
6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7
6.1 FASE DE DIAGNOSTICO DEL MSPI 8
6.1.1 ESTADO ACTUAL DE LA ENTIDAD 9
6.1.2 BRECHA ANEXO A - ISO 27001:2013 10
6.1.3 CICLO PHVA 11
6.2 FASE DE PLANEACIÓN 13
6.2.1 PLAN DE SEGURIDAD DE LA INFORMACIÓN 14
6.2.2 POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 14
6.2.3 OBJETIVOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 15
6.2.4 ROLES Y RESPONSABILIDADES 15
6.2.5 INVENTARIO ACTIVOS DE INFORMACIÓN 15
6.2.6 INTEGRACIÓN MSPI CON EL SISTEMA DE GESTIÓN DOCUMENTAL 22
6.2.7 IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGO 22
6.2.8 PLAN DE COMUNICACIONES 22

COPIA CONTROLADA

6.3 FASE DE IMPLEMENTACIÓN 23

6.3.1 PLANIFICACIÓN Y CONTROL OPERACIONAL 23

6.3.2 IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO 23

6.3.3 INDICADORES DE GESTIÓN 24

6.4 FASE DE EVALUACIÓN DE DESEMPEÑO 25

6.4.1 PLAN DE REVISIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DE MSPI 25

6.4.2 PLAN DE EJECUCIÓN DE AUDITORIAS 26

6.5 FASE DE MEJORA CONTINUA 26

7. MODELO DE MADUREZ 27

8. ADOPCIÓN DEL PROTOCOLO IPV6 27

8.1 FASE DE PLANEACIÓN 27

8.2 FASE DE IMPLEMENTACIÓN 28

8.3 PRUEBAS DE FUNCIONALIDAD 28

9. NORMAS 29

10. DOCUMENTOS DE REFERENCIA 29

COPIA CONTROLADA

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 27001:2013 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 2013, 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 27001:2013 garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

COPIA CONTROLADA

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

COPIA CONTROLADA

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

Activo: Cualquier cosa que tenga valor para la organización. [ISO 27001:2005]

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: 2016].

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: 2012].

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 27001:2005]

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [ISO/IEC 27000: 2016]

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: 2016].

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: 2016].

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 - 100.05.25.D.32 – 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: 2016].

SGI: Sistema Integrado de Calidad [Institución Universitaria Colegio Mayor del Cauca]

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

COPIA CONTROLADA

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.

COPIA CONTROLADA

[1] Modelo de Seguridad y Privacidad de la Información _ MINTIC. https://www.mintic.gov.co/gestionti/615/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

COPIA CONTROLADA

DIAGNOSTICO			
METAS	Actividades/Instrumentos	TIEMPO ESTIMADO	RESULTADOS
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Institución Universitaria	Diligenciamiento del Instrumento Evaluación MSPI emitido por MINTIC.	17/01/2022 - 30/12/2022	Instrumento Evaluación MSPI con la valoración del 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 en Línea.		
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.	01/11/2022 - 30/12/2022	Declaración de Aplicabilidad. Riesgos actualizados

COPIA CONTROLADA

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 79 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	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	82	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	78	100	GESTIONADO
A.9	CONTROL DE ACCESO	71	100	GESTIONADO
A.10	CRIPTOGRAFÍA	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	74	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	79	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	78	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	80	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	70	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	86	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	85	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**79**	**100**	GESTIONADO

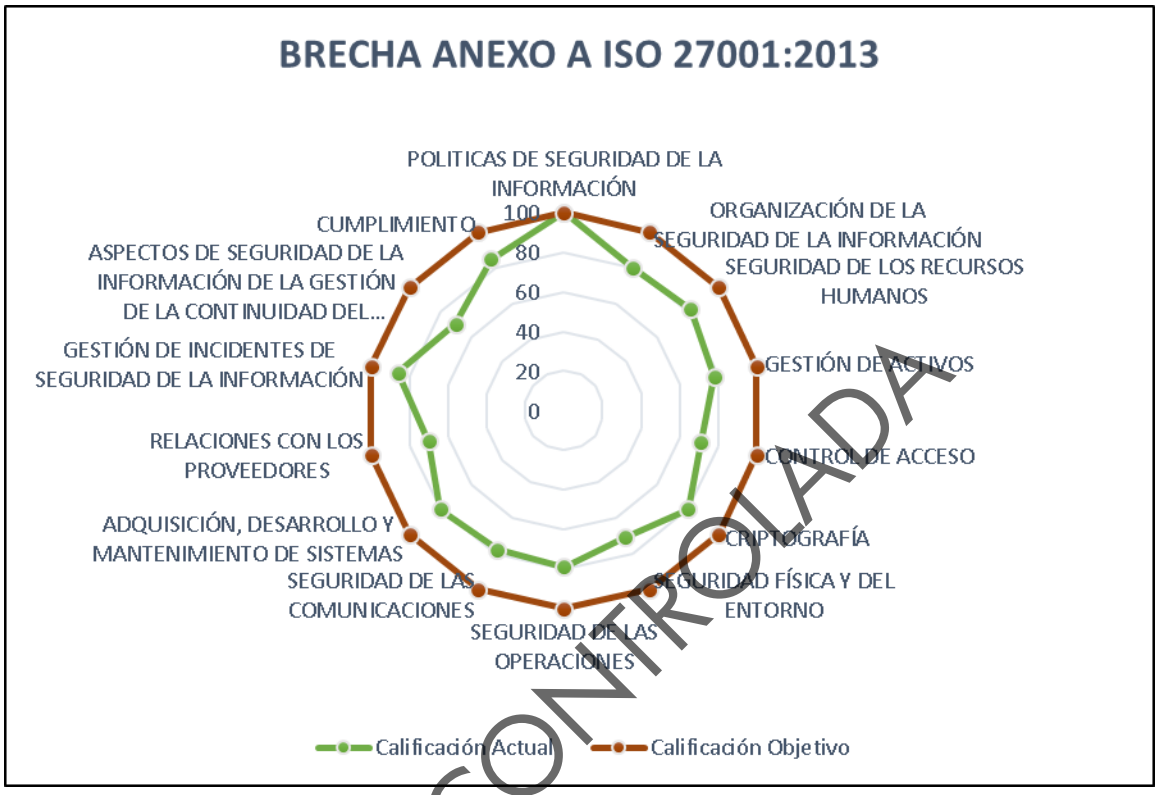
COPIA CONTROLADA

Se deben MEJORAR los controles A.9. Control de acceso, A.11. Seguridad física y del entorno, A.15. Relaciones con los proveedores y A.17. Aspectos de seguridad de la información de la gestión de la continuidad del negocio 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 27001:2013 en su anexo A.

6.1.2 BRECHA ANEXO A - ISO 27001:2013

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 27001:2013), los activos que la contienen y los medios relacionados.

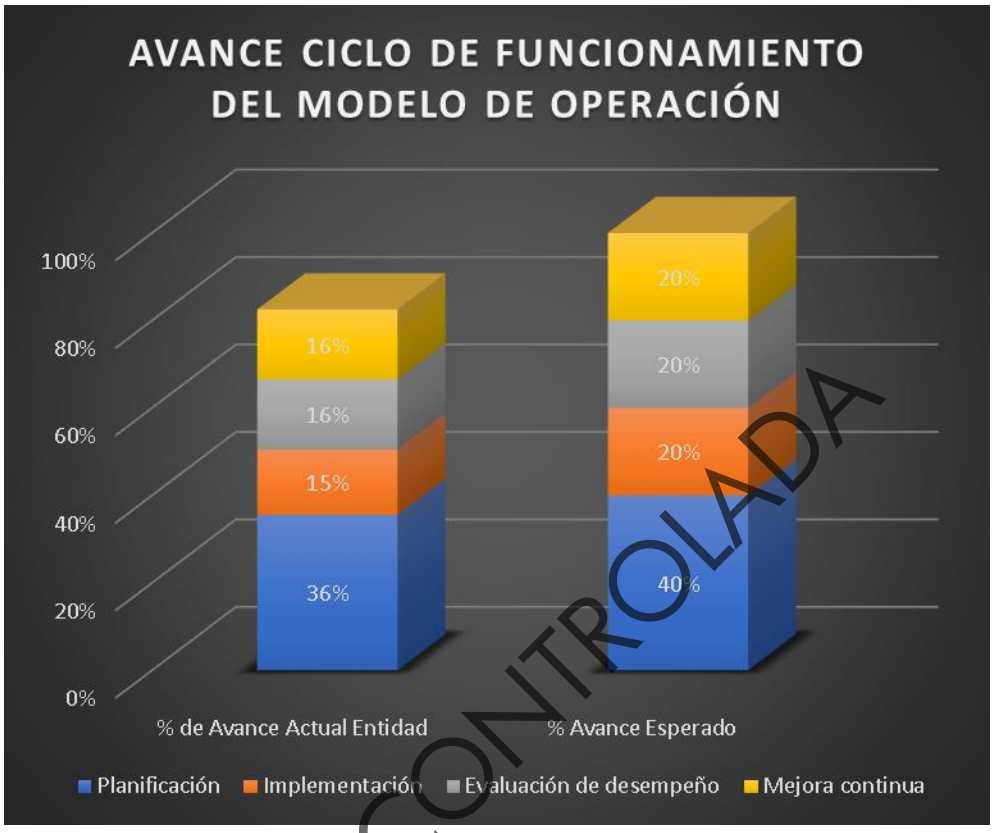
La brecha encontrada, se puede apreciar en la siguiente gráfica, evidenciando el riesgo al que se encuentra expuesta la información.



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).

COPIA CONTROLADA



COPIA CONTROLADA

Identificamos un avance del 36% referente a la PLANIFICACIÓN y el 15% en la fase de IMPLEMENTACIÓN, un avance de 16% las fases de EVALUACIÓN DE DESEMPEÑO y MEJORA CONTINUA.

Los resultados obtenidos del cumplimiento de la norma ISO/IEC: 27001:2013 se representan de manera general en el siguiente grafico

Año	AVANCE PHVA		
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
1	Planificación	36%	40%
2	Implementación	15%	20%
3	Evaluación de desempeño	16%	20%
4	Mejora continua	16%	20%
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 SGI (Sistema de Gestión Integrado) y el plan de tratamiento de riesgos de seguridad y privacidad de la información.

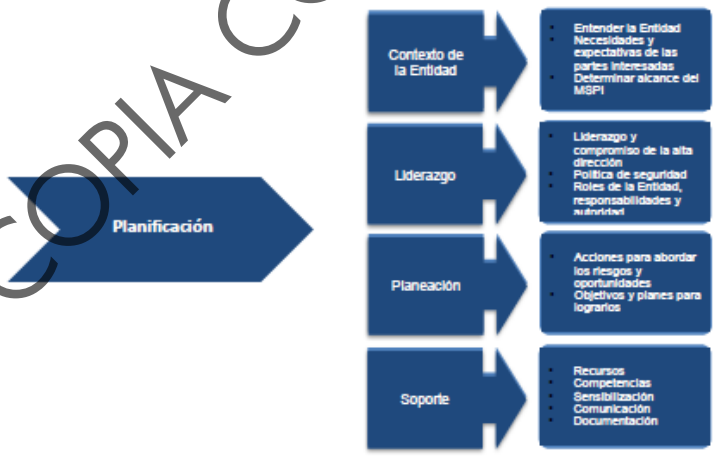


Figura 3. Fase de planificación[2]

COPIA CONTROLADA

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

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.	17/01/2022 - 30/12/2022	Política de seguridad y privacidad de la información.
	Generar guía de políticas de seguridad y privacidad de la información, aprobado por la dirección.		Guía de normas y buenas prácticas en seguridad y privacidad de la información.
	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.	Actualizar documento roles y responsabilidades del comité de seguridad (o quien haga sus veces)	17/01/2022 - 30/12/2022	Documento roles y responsabilidades del comité se seguridad y privacidad aprobado y publicado en SGI.
Inventario activo de información y gestión de riesgos.	Actualización inventario activos de información de acuerdo al plan de tratamiento de riesgo.	17/01/2022 - 30/12/2022	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	17/01/2022 - 30/12/2022	Documentos o procedimientos actualizados

COPIA CONTROLADA

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 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 104.01.02.D.12 Roles Y Responsabilidades Seguridad De La Información, disponible en el link https://campus.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 (SGI)	Responsable
[S] SERVICIOS			
1.	[S_ACADEMICO_ADMINISTRATIVO] Servicios CAMPUS	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
2.	[S_WEB]	Comunicaciones	Web master P.U. Comunicaciones Contratista Externo

COPIA CONTROLADA

		Gestión de Recursos Tecnológicos	
3.	[S_WIFI]	Gestión Recursos Tecnológicos	P.U Seguridad Digital
4.	[S_CORREO_ELECTRONICO]		P.U Seguridad Digital
5.	[S_TELFONIA_IP]		P.U Seguridad Digital
6.	[S_DHCP]		P.U Seguridad Digital
7.	[S_MAQUINAS_V]		P.U Seguridad Digital
8.	[S_ANTIVIRUS]		P.U Seguridad Digital
9.	[S_SNIES]	Gestión Recursos Tecnológicos	P.U Seguridad Digital
10.	[S_CAMARAS_IP]	Gestión Recursos Tecnológicos	P.U Seguridad Digital
11.	[S_FINANCIERO]	Gestión Financiera y Contable	P.U Seguridad Digital
12.	[S_CATALOGO_BIBLIOTECA]	Gestión de Biblioteca	Bibliotecólogo
13.	[S_MOODLE]	Gestión Recursos Tecnológicos	P.U Seguridad Digital
14.	[S_DNS]	Gestión Recursos Tecnológicos	P.U Seguridad Digital
15.	[S_BACKUPS]	Gestión Recursos Tecnológicos	P.U Seguridad Digital
16.	[S_SITH] (Sistema Información Talento Humano)	Gestión de Talento Humano	P.U de Talento Humano Gestión Recursos Tecnológicos
17.	[S_Inventario_Incidencias]	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos
18.	[INFO_R] Información restringida	Gestión Documental	P.U. Gestión Documental
19.	[INFO_PUBLICA]	Gestión Documental	P.U. Gestión Documental
[S] APLICACIONES (Software)			
20.	[S_CAMPUS_AA] CAMPUS Academico – Administrativo	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
21.	[S_ SICCED_DA]Sistema de Evaluación Docente – Alumnos	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software

COPIA CONTROLADA

22.	[S_ SICCED_DD]Sistema de Evaluación Docente – Decano	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
23.	[S_ SICCED_V]Sistema de Evaluación Docente -Vicerrector	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
24.	[S_ CAMPUS _R] CAMPUS Reporte [Administrativos]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
25.	[S_ CAMPUS _P] CAMPUS Promedio MVC – Facultades	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
26.	[S_ CAMPUS _ BU] CAMPUS Bienestar Universitario	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
27.	[S_S CAMPUS _RN_PR] CAMPUS Registro de Notas programas Regulares	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
28.	[S_ CAMPUS _CN-PR] CAMPUS Consulta de Notas Programas Regulares.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
29.	[S_ CAMPUS _RL_PR] CAMPUS Registro en Línea Programas Regulares	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
30.	[S_ CAMPUS _L] CAMPUS Liquidación [Recaudos - Certificados]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
31.	[S_ CAMPUS _RL] Sistema de Información Académico Extensión Registro en Línea.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
32.	[S_ CAMPUS AA] CAMPUS Admisiones para Administrativos de Admisiones	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software. Director Admisiones.
33.	[S_FACTURA_I] Factura de Inscripción Aspirantes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
34.	[S_ CAMPUS AC] CAMPUS Académico para administrativos Ingles.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
35.	[S_ CAMPUS RN] CAMPUS Registro Notas Ingles	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
36.	[S_ CAMPUS _CN] CAMPUS Consulta de Notas	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
37.	[S_ CAMPUS _G] CAMPUS Registro Graduandos.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
38.	[S_ CAMPUS _Adm] CAMPUS para Personal de Desarrollo.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
39.	[S_Task_Manager] Registro de actualizaciones de software personal TIC	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
40.	[S_ CAMPUS _EGRESADOS] CAMPUS Administrativo Egresados	Administrativo-Admisiones	P.U. Desarrollo de Software. Responsable Egresados
41.	[S_ CAMPUS _BA_I] CAMPUS Bienestar _ ICETEX	Casa Obando	P.U. Desarrollo de Software. Asesor Bienestar
42.	[S_ CAMPUS _BIBLIOTECA] CAMPUS Registro Multas de Biblioteca.	Bienestar Institucional	P.U. Desarrollo de Software.

COPIA CONTROLADA

			P.U. Biblioteca
43.	[S_ CAMPUS_REG_N_D] Registro de Notas Extensión [Docentes Inglés]	Docentes Ingles	P.U. Desarrollo de Software
44.	[S_SGI] Sistema de Gestión Integrado	Egresados	P.U. Desarrollo de Software
45.	[S_Acciones] Sistena de Acciones y Mejoras	Docencia	P.U. Desarrollo de Software
46.	[S_HELPDESK] Sistema Inventario e Incidencias de Activos de TI	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
47.	[S_Ponderados] Sistema de Ponderados UNIMAYOR	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
48.	[S_PQR´S] Sistema Web de PQR´S	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
49.	[S_Directorio] Sistema Web Directorio Institucional	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
50.	[S_ CAMPUS _ME] CAMPUS Modulo Externo de Egresados	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Contratista Egresados
51.	[S_ CAMPUS _MF] CAMPUS matricula Financiera Admisiones - Aspirantes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
52.	[S_ CAMPUS _SNIES] CAMPUS Reporte a SNIES	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Auxiliar Vicerrectoria
53.	[S_ CAMPUS _Electoral] CAMPUS Elección Representantes Entes Institucionales	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Secretaria General
54.	[S_ CAMPUS _Bitácoras] CAMPUS reporte actividades Docentes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
55.	[S_Utility] Sistema registro actividades Personal Desarrollo	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
56.	[S_ CAMPUS _INV] CAMPUS Investigaciones	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Contratista Investigaciones
57.	[S_R_FISICOS] CAMPUS Recursos Físicos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos
58.	[S_ CAMPUS _INT] CAMPUS Internacionalización	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos P.U. Internacionalización
59.	[S_ CAMPUS _LR] CAMPUS Liquidación Recaudos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Aux-Facultades
60.	[S_ CAMPUS _MFA] CAMPUS Matriculas Financieras Admisiones - Aspirantes	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Director Admisiones

COPIA CONTROLADA

61.	[S_ CAMPUS_PS] CAMPUS Proyección Social	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Responsable Proyección Social
62.	[S_ CAMPUS _BP] CAMPUS Banco de Proyectos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Jefe Oficina Asesora Planeación
63.	[S_ CAMPUS _G] CAMPUS Graduandos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Responsable Egresados
64.	[S_Consulta_F] Sistema Consulta Financiera	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Aux-Facultades
65.	[S_Recursos_T] Sistema de Recursos Tecnológicos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos
66.	[S_ CAMPUS _Ambiental] Sistema Ambiental	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Contratista Ambiental
67.	[S_RESERVAS] Sistema de Reservas de Salas de Reunión	Gestión Recursos Tecnológicos	Contratista TIC
68.	[S_AGENDA] Sistema de Agenda Institucional	Gestión Recursos Tecnológicos	Contratista TIC
69.	[S_SAEVA]Sistema de Autoevaluación	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
70.	[S_ENC] Sistema de Encuestas Unimayor	Gestión Recursos Tecnológicos	Contratista Desarrollo de Software
71.	[S_SITH] Sistema de Talento Humano	Gestión y Desarrollo del Talento Humano	Gestión y Desarrollo del Talento Humano
72.	[S_UNICA] Sistema de Unidad de Correspondencia	Gestión Documental	Contratista Unidad de Correspondencia
73.	[S_CELESTE] Sistema Contable y Financiero	Dirección Financiera y Contable	Director(a) Financiero(a) y Contable
74.	[S_CATALOGO_BIBLIOTECA] Sistema Integrado de Gestión de Bibliotecas	Gestión de Biblioteca	Bibliotecólogo
[HW] EQUIPOS INFORMÁTICOS (Servidores, Hardware)			
75.	[SER_BCP_CAMPUS] Servidor Business Continuity Plan del CAMPUS	Gestión Recursos Tecnológicos	P.U Seguridad Digital
76.	[SER_SIAG] Servidor Sistema de Información Académica y Gestión	Gestión Recursos Tecnológicos	P.U Seguridad Digital

COPIA CONTROLADA

77.	[SER_WEB_BACKUPS] Servidor Sitios Web	Gestión Recursos Tecnológicos	P.U Seguridad Digital
78.	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	P.U Seguridad Digital
79.	[SER_ANTIVIRUS] Servidor Antivirus y Máquinas Virtuales	Gestión Recursos Tecnológicos	P.U Seguridad Digital
80.	[SER_SNIES] Servidor SNIES	Gestión Recursos Tecnológicos	P.U Seguridad Digital
81.	[SER_CAM_P] Servidor Cámaras IP, Pantallas Informativas y Aplicaciones WEB	Gestión Recursos tecnológicos	P.U Seguridad Digital
82.	[SER_CELESTE] Servidor Sistema Financiero y Contable	Gestión Recursos Tecnológicos	P.U Seguridad Digital
83.	[SER_CATALOGO_BIBLIOTECA] Servidor Catálogo Biblioteca	Gestión de Biblioteca	Bibliotecólogo
84.	[SER_MOODLE_DNS] Servidor Herramientas Virtuales de Aprendizaje	Gestión Recursos Tecnológicos	P.U Seguridad Digital
85.	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	P.U Seguridad Digital
86.	[HW_PC] Equipos de cómputo (escritorio y portátiles)	Todos	Todos
87.	[HW_IMP] Impresoras	Administrativos – Docentes	Todos
88.	[HW_ESC] Escáneres	Administrativos – Docentes	Todos
89.	[HW_SWIT] Switch administrable	Gestión Recursos Tecnológicos	P.U Seguridad Digital
90.	[HW_FW] Firewall UTM	Gestión Recursos Tecnológicos	P.U Seguridad Digital
91.	[HW_WAP] Punto de Acceso Inalámbrico	Gestión Recursos Tecnológicos	P.U Seguridad Digital
92.	[HW_enrutadores] Enrutadores	Gestión Recursos Tecnológicos	Proveedor ISP
93.	[HW_Radio_Enlace] Radio Enlace Interconexión Alterna	Gestión Recursos Tecnológicos	P.U Seguridad Digital
94.	[HW_Gateway] Gateway VoIP	Gestión Recursos Tecnológicos	proveedor ISP
[COM] Redes de Comunicaciones			
95.	[COM_RT] Red Telefónica	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos

COPIA CONTROLADA

96.	[COM_Datos] Red de Datos	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
97.	[COM_WIFI] Red inalámbrica	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
98.	[COM_MAN] Red Area Metropolitana	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
99.	[COM_ISP] Internet	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
[SI] SOPORTES INFORMACIÓN			
100	[SI_CD_ROM/DVD] Soportes de información en CD-ROOM y/o DVD	Todos	Todos
101	[SI_USB] Soportes de información en Discos Externos USB	Todos	Todos
102	[SI_IMPRESOS] Soportes de Información Impresos en Papel	Todos	Todos
103	[SI_NAS] Almacenamiento en la Red	Gestión Recursos Tecnológicos	Todos
104	[SI_AA] Almacenamiento de archivos en nube Privada	Gestión Recursos Tecnológicos	Todos
105	[SI_Drive] Almacenamiento en la Nube (Gmail)	Todos	Todos
[AUX] EQUIPAMIENTO AUXILIAR			
106	[AUX_UPS] Sistema de Alimentación Ininterrumpida	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
107	[AUX_AC]Aires Acondicionados	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
108	[AUX_Cabl_Elect] Cableado Eléctrico	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
109	[AUX_Cabl_Datos] Cableado Datos	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
110	[AUX_DEST] Equipo Destrucción de Papel	Gestión Documental	P.U. Gestión Documental
111	[AUX_CF] Cajas Fuertes	Gestión Contable y Financiera	Director(a) Financiero(a) y Contable
112	[AUX_Tel] Teléfonos	Gestión Recursos Tecnológicos	Todos
113	[AUX_VIG] Cámaras de Vigilancia	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
[L] INSTALACIONES			
114	[L_Edificio] Edificios		
115	[L_DATOS] Centros de Datos	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
116	[L_CANAL] Canalización (Cableados)	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos

COPIA CONTROLADA

117	[L_GAB] Gabinete de red	Gestión Recursos Tecnológicos	Director Gestión de Recursos Tecnológicos
[P] PERSONAL			
118	[P_UE] Usuarios Externos	Talento Humano	P.U. Talento Humano
119	[P_UI] Usuarios Internos	Talento Humano	P.U. Talento Humano
120	[P_ADM] Administradores de Sistemas	Gestión Recursos Tecnológicos	Desarrolladores
121	[P_DBA] Administrador de Bases de Datos	Gestión Recursos Tecnológicos	Desarrolladores
122	[P_SEC] Administradores de seguridad	Gestión Recursos Tecnológicos	Desarrolladores
123	[P_DES] Desarrollo Software	Gestión Recursos Tecnológicos	Desarrolladores
124	[P_CON] Contratistas	Talento Humano	P.U. Talento Humano
125	[Proveedores] Proveedores	Talento Humano	P.U. Talento Humano
126	[P_OCA] Ocasionales	Talento Humano	P.U. Talento Humano

COPIA CONTROLADA

6.2.6 INTERACIÓN 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 104.01.02.D.14 Plan de Tratamiento de Riesgos de seguridad y privacidad de la información disponible en:

https://unimayor.edu.co/web/transparencia?layout=edit&id=2856#ano-2022; 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 104.01.02.D.13 Plan de sensibilización seguridad de la información, disponible en: https://campus.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:

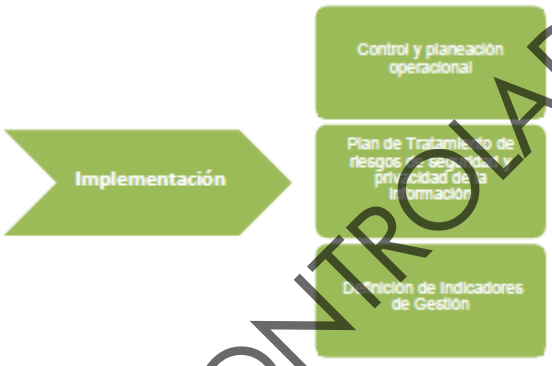


Figura 4. Fase de implementación

COPIA CONTROLADA

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 2022, las acciones (controles) deben estar registradas según los formatos existentes en el SGI o aplicativo destinado para tal fin, de igual manera deberá acoger lo estipulado en el procedimiento 106.20.03.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.

COPIA CONTROLADA

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	Backup 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

Proceso	Nombre	Objetivo del indicador	Fórmula	Meta	Periodicidad de medición	Responsable de cumplir la meta
Líderes de proceso	Cumplimiento auditorías internas del SGSI	Conseguir y mantener nivel de compromiso con la seguridad por parte de empleados y contratistas.	# de acciones correctivas implementadas / # de hallazgos de auditoría	80%	Anual	Líder de Seguridad

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:

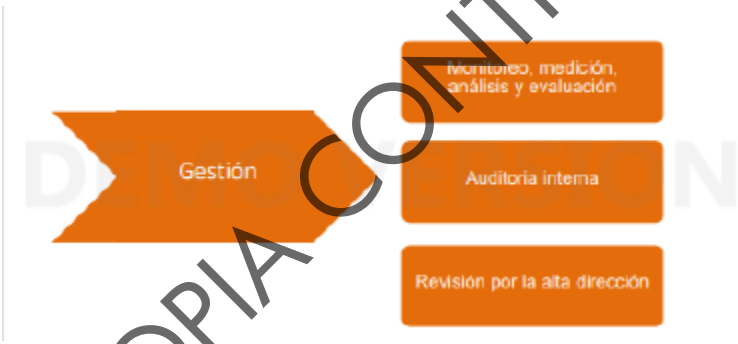


Figura 5. Fase de Evaluación y Desempeño

COPIA CONTROLADA

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.	Semestral
Seguimiento a la programación y ejecución de las actividades de auditorías internas y externas del MSPI	Una vez al año

Seguimiento al alcance y a la implementación del MSPI.	Una vez al año
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.	Semestral
Revisión de indicadores de gestión de seguridad de la información	Semestral
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 105.02.07.P.03 PROCEDIMIENTO AUDITORÍAS, disponible en: https://campus.unimayor.edu.co/CampusSGI opción: Campus Unimayor SAIC/Evaluación y Seguimiento/Evaluación y seguimiento/Procedimientos, 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.

COPIA CONTROLADA

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.

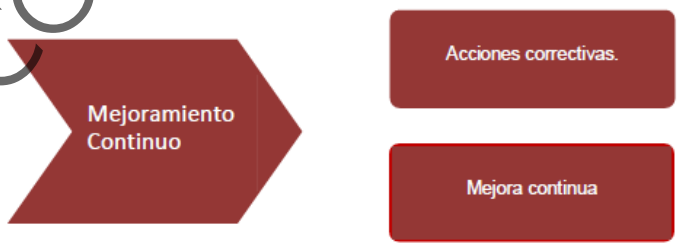


Figura 6. Fase de Mejora Continua

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 Continua tomando como referencia el procedimiento 106.20.03.P.03 ACCIONES CORRECTIVAS, PLANES DE MEJORAMIENTOY SALIDAS NO CONFORMES

(https://campus.unimayor.edu.co/CampusSGI opción: Campus Unimayor SAIC/Evaluación y Seguimiento/Evaluación y seguimiento/Procedimientos)

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 144 controles agrupados en 14 dominios descritos en el anexo A de la norma ISO/IEC 27001:2013, además de los requerimientos del Instituto Nacional de Patrones y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology) obtuvimos una calificación del 79% lo que nos da la clasificación de "GESTIONADO"; como se detalla en la siguiente gráfica:

COPIA CONTROLADA

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	82	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	78	100	GESTIONADO
A.9	CONTROL DE ACCESO	71	100	GESTIONADO
A.10	CRIPTOGRAFÍA	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	71	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	79	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	78	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	80	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	70	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	86	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	85	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**79**	**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.

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.

COPIA CONTROLADA

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).

COPIA CONTROLADA

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 Diagnostico de Seguridad y Privacidad.

104.01.02.P.07 Procedimiento Para Continuidad Del Negocio.

104.01.02.R.24 Formato Declaración De Aplicabilidad

104.01.02.P.09 Gestión De Incidentes De Seguridad De La Información.

100.05.05.D.39 Política, alcance y objetivos de seguridad de la información.

104.01.02.D.12 Roles Y Responsabilidades Seguridad De La Información.

104.01.02.D.13 Plan De Sensibilización Seguridad De La Información

100.05.05.D.40 Política De Seguridad De La Información Control De Acceso.

100.05.05.D.41 Política De Seguridad De La Información Desarrollo Seguro.

100.05.05.D.42 Política De Seguridad De La Información Gestión De Los Activos De Información.

100.05.05.D.43 Política De Seguridad Para Proveedores.

104.01.02.D.20 Plan De Seguridad Y Privacidad De La Información.

104.01.02.D.14 Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información.

104.01.02.R.23 Formato de Incidente De Seguridad De La Información.

202.02.01.P.01 Convocatoria, Selección, Vinculación Y Retiro De Personal

202.03.03.P.04 Formación Y Capacitación Del Personal

106.20.03.P.03 Acciones Correctivas, Planes De Mejoramiento y Proyectos de mejora

106.20.03.P.01 Control De Documentos.

105.02.07.P.03 Procedimiento Auditorías

COPIA CONTROLADA

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.
6 de septiembre de 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 de octubre de 2022	Se actualiza el Plan de seguridad según revisión realizada por el proceso de Gestión de Recursos Tecnológicos.

COPIA CONTROLADA