PLAN DE TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
_____	_____	_____
Contratista Seguridad y privacidad de la información	Asesor TIC	Rector(a)

CONTENIDO

1. INTRODUCCION 3
2. OBJETIVOS 3
   2.1. GENERAL 3
   2.2. ESPECIFICOS 3
3. ALCANCE 3
4. TÉRMINOS Y DEFINICIONES 4
5. ANALISIS DE CONTEXTO ESTRATEGICO (DOFA) 5
6. PLAN DE ACCION DE GESTION DE RIESGO 8
   6.1. TIPO DE ACTIVOS: 9
   6.2. IDENTIFICACIÓN Y ANALISIS DE RIESGOS 22
7. SEGUIMIENTO A CONTROLES DE RIESGOS 22
8. PLAN DE CONTINUIDAD DEL NEGOCIO 22
9. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 22
10. PLAN DE CAPACITACIÓN 23
11. MARCO LEGAL 23
12. BIBLIOGRAFIA 24
13. CONTROL DE CAMBIOS 24

1. INTRODUCCION

La gestión de riesgos de seguridad y privacidad de la información permite realizar la detección temprana de vulnerabilidades, amenazas y/o debilidades minimizando perdida de información y asegurando la continuidad de los procesos.

La Institución Universitaria Colegio Mayor del Cauca certificada con los estándares ISO 9001:2015, NTC 5555:2011 y NTC 5580:2011, entiende la necesidad de implementar el plan estratégico de gestión de riesgo de seguridad y privacidad de la información basado en el estándar ISO/IEC 27001:2013 articulado con el Sistema de Gestión Integrado garantizando la confidencialidad integridad y disponibilidad de la información.

2. OBJETIVOS

2.1. GENERAL

Implementar el plan de gestión de riesgo de seguridad y privacidad de la información, articulado con los requerimientos de Gobierno Digital y MIPG tomando como plataforma la ISO/IEC 27001:2013.

2.2. ESPECÍFICOS

1. Alinear los procesos del Sistema de Gestión Integrado (SGI) con los controles del Sistema de Gestión de Seguridad de la Información, descritos en el Anexo A de la norma ISO 27001:2013.
2. Definir el alcance y delimitación del Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información.
3. Mantener actualizados los activos de información relevantes de la Institución Universitaria Colegio Mayor del Cauca.
4. Monitorear los incidentes de seguridad de la información detectados como críticos y realizar la gestión.

3. ALCANCE

El plan de Riesgos de Seguridad y Privacidad de la información aplica a todos los procesos de la institución Universitaria Colegio Mayor del Cauca los cuales manejen, procesen o interactúen con información tanto física como digital.

4. 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 27001:2005]
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]
DECLARACIÓN DE APLICABILIDAD (SOA- Statement Of Applicability): Documento que contiene los controles del Sistema de Gestión de Seguridad de la Información, requisito de la ISO/IEC 27001.
DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [ISO/IEC 27000: 2016].
DISRUPCIÓN O INTERRUPCIÓN: Evento o circunstancia que puede afectar significativamente las operaciones críticas de la organización. Esto incluye cualquier ocurrencia inesperada de causa natural, técnica o humana. [ISO/IEC 22301: 2012].
DOFA: Método de planificación que permite conocer el estado actual de una empresa, permitiendo buscar soluciones para sus aspectos negativos, logrando así la mejoría progresiva del negocio.
EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. [Guía ISO/IEC 73:2002].
IMPACTO: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo. [Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP octubre 2018].
INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento o serie de eventos inesperados o no deseados de seguridad de la información con probabilidad significativa que puede afectar las operaciones del negocio y amenazar la seguridad de la información.

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].

IUCMC: Abreviatura de Institución universitaria Colegio Mayor del Cauca

NO CONFORMIDAD: Incumplimiento de un requisito, política o documento, cuya repetición pone en riesgo la efectividad.

POLÍTICA: Intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000: 2016].

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 - 100.01.01.01.P.02 – SGI Colegio Mayor del Cauca).

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

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].

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI): 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.

5. ANÁLISIS DE CONTEXTO ESTRATÉGICO (DOFA)

Se realizó análisis de seguridad y privacidad de la información haciendo uso de la matriz DOFA, para determinar el estado actual, con el propósito de identificar riesgos e implementar controles que garanticen la continuidad del negocio.

ANÁLISIS INTERNO		ANÁLISIS EXTERNO	
FORTALEZAS	DEBILIDADES	OPORTUNIDADES	AMENAZAS

El Sistema de Gestión de Seguridad de la Información cuenta con documentos aprobados para el tratamiento de riesgos.	Falta de articulación entre los sistemas de información, que pueden desencadenar reproceso o pérdida de información.	Articular proyectos de innovación tecnológica y seguridad informática para lograr trabajo colaborativo y satisfacción de necesidades de las partes interesadas.	Respuesta no inmediata (parcial o total), por parte de los proveedores externos, materializados en pérdida o cambios que afecten la información.
Uso de infraestructura tecnológica pertinente para mitigar riesgos de seguridad y privacidad de la información tal como el UTM (Sistema Unificado contra Amenazas), sistema de protección contra malware y virus y el sistema de backups automatizado.	No contar con la disponibilidad de un ambiente de producción y un ambiente de pruebas para el desarrollo e implementación de software y sistemas de información.	Mejorar el nivel de cumplimiento a los requerimientos de gobierno por parte de los entes de control en términos de seguridad y privacidad de la información.	Ataques híbridos (Ingeniería social e informáticos) contra los funcionarios y/o empleados que generen impactos sobre la institución.
Se cuenta con la madurez de un sistema de gestión de calidad en la Institución, el cual puede ser integrado con el SGSI actual.	Deficiencia de la comunicación interna.	Generar, actualizar y divulgar políticas, documentos y procedimientos relacionados con Seguridad y Privacidad de la Información.	Incumplimiento en el mantenimiento contratado con personal externo.
La creación del comité liderado desde la Alta Dirección para la revisión y aceptación de la estructura del SGSI desde su	No se cuenta con un procedimiento formal exactamente de un plan de contingencia general para enfrentar incidentes de seguridad de la información.	Proyectos de mejora encaminados al diseño, implementación y mantenimiento de controles a nivel de infraestructura	Daño en equipos o medios tecnológicos.

planeación hasta la mejora continua.		tecnológica para el aseguramiento de la información institucional.	
Servidores Privados Virtuales (VPS), con el fin de mantener en alto grado de disponibilidad los servicios críticos tales como página web institucional y SIAG como parte de implementación del plan de continuidad de negocio.	Datos incompletos, incorrectos, inexactos o no pertinentes en las bases de datos institucionales.	Llevar a cabo pruebas a los controles implementados de forma periódica siguiendo las mejores prácticas para la Seguridad y Privacidad de la Información.	Nuevas regulaciones gubernamentales que obliguen a cambiar la operación de la Institución.
Mejoras encaminadas a la instalación, re-estructuración y montaje de la red de datos, red eléctrica y dispositivos tecnológicos además de mejoras en el diseño de seguridad perimetral y unificación de la red.	No contar con espacios y puestos de trabajos adecuados y/o restringidos si se maneja información sensible para el desarrollo de las actividades.		Afectación de servicios tecnológicos debido a fenómenos meteorológicos, medioambientales o eventos externos.
Articulación de proyectos de grado relacionados con Seguridad y Privacidad de la Información con la Facultad de Ingeniería, aplicados a la institución sobre	Falencia en la implementación y aprobación de la política de control de acceso (Identificación única, niveles de acceso y privilegios en sistemas de información, sistemas de cifrado, sitios de		Hurto de activos de información.

los activos de información.	acceso a solo personal autorizado etc.)		
	No se tienen establecido un procedimiento de disposición final de equipos de cómputo, información en medios digitales e información o documentación física.		
	Ausencia de controles efectivos para prevenir la instalación de software no autorizado en la institución.		
	No se cuenta con una política o procedimiento para la administración de equipos móviles (Portátiles, Cámaras, Dispositivos de almacenamiento, Celulares) que contengan información institucional.		

Tabla 1. DOFA IUCMC

6. PLAN DE ACCIÓN DE GESTIÓN DE RIESGO

Teniendo claramente definido el contexto, se identificaron y clasificaron los activos de información tanto física como digital presente en cada uno de los procesos críticos Institucionales, tomando como referencia la norma ISO/IEC 270001:2013.

6.1. TIPO DE ACTIVOS:

Los activos de información deben ser identificados por los líderes de proceso o responsables de los activos y del responsable de seguridad de la información, teniendo en cuenta la siguiente clasificación:

No.	Id Activo/Clasificación	Proceso /Sub-Proceso (SGI)	Responsable	Perfiles Usuario
[S] SERVICIOS				
1.	[S_SIAG] Servicios SIAG	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	NA
2.	[S_WEB]	Comunicaciones y TIC	Web master P.U. Comunicaciones Contratista Externo	
3.	[S_WIFI]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
4.	[S_CORREO_ELECTRONICO]		T.A. Red Datos y Servidores	
5.	[S_TELFONIA_IP]		T.A. Red Datos y Servidores	
6.	[S_DHCP]		T.A. Red Datos y Servidores	
7.	[S_MAQUINAS_VI]		T.A. Red Datos y Servidores	
8.	[S_ANTIVIRUS_ESET]		T.A. Red Datos y Servidores	
9.	[S_SNIES]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
10.	[S_CAMARAS_IP]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
11.	[S_SICOF]	Gestión Financiera y Contable	T.A. Red Datos y Servidores	
12.	[S_SIABUC_WEB]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	

13.	[S_SIABUC_LOCAL]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
14.	[S_MOODLE]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
15.	[S_DNS]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
16.	[S_BACKUPS]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
17.	[S_SITH] (Sistema Información Talento Humano)	Gestión de Talento Humano	P.U. de Talento Humano Gestión Recursos Tecnológicos	
18.	[S_Inventario_Incidencias]	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos	
19.	[INFO_R] Información restringida	Gestión Documental	P.U. Gestión Documental	
20.	[INFO_PUBLICA]	Gestión Documental	P.U. Gestión Documental	
[S] APLICACIONES (Software)				
21.	[S_SIAG_AA] SIAG Académico –Administrativo	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Auxiliares administrativas de cada facultad. Permisos: Edición y consulta.
22.	[S_ SICCED_DA]Sistema de Evaluación Docente – Alumnos	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Estudiantes de programas regulares IUCMC. Permisos: Registro.
23.	[S_ SICCED_DD]Sistema de Evaluación Docente – Decano	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Decanos de cada facultad. Permisos: Registro y consulta.

24.	[S_ SICCED_V]Sistema de Evaluación Docente - Vicerrector	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Vicerrector IUCMC. Permisos: Registro y consulta.
25.	[S_SIAG_R] SIAG Reportes [Administrativos]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Personal académico-administrativo IUCMC. Permisos: consulta.
26.	[S_SIAG_P] SIAG Promedio MVC – Facultades	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Auxiliares administrativas de cada facultad. Permisos: consulta.
27.	[S_SIAG_ BU] SIAG Bienestar Universitario	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Personal administrativo oficina bienestar universitario IUCMC. Permisos: consulta.
28.	[S_SIAG_RN_PR] SIAG Registro de Notas programas Regulares	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Docentes programas regulares IUCMC. Permisos: registro, edición y consulta.
29.	[S_SIAG_CN-PR] SIAG Consulta de Notas Programas Regulares.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Estudiantes de programas regulares IUCMC. Permisos: consulta.

30.	[S_SIAG_RL_PR]SIAG Registro en Línea Programas Regulares	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Aspirantes de programas regulares IUCMC. Permisos: registro, edición y consulta.
31.	[S_SIAG_L] SIAG Liquidación [Recaudos - Certificados]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Auxiliares administrativas de cada facultad. Permisos: registro, edición y consulta.
32.	[S_SIRAEX_RL] Sistema de Información Académico Extensión Registro en Línea.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Aspirantes de programas ingles IUCMC. Permisos: registro, edición y consulta.
33.	[S_SIRAEX_AA] SIRAEX Admisiones para Administrativos de Admisiones	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software. Asesor Admisiones.	Personal administrativo oficina admisiones IUCMC. Permisos: registro, edición y consulta.
34.	[S_FACTURA_I] Factura de Inscripción Aspirantes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Aspirantes de programas IUCMC. Permisos: registro y consulta.
35.	[S_SIRAEX_AC]SIRAEX Académico para administrativos Ingles.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Personal administrativo del programa de inglés IUCMC.

				Permisos: Registro y consulta.
36.	[S_SIRAEX_RN] SIRAEX Registro Notas Ingles	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Docentes del programa de inglés. Permisos: registro, edición y consulta.
37.	[S_SIRAEX_CN] SIRAEX Consulta de Notas	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Estudiantes de programas de inglés. Permisos: consulta.
38.	[S_SIAG_G] SIAG Registro Graduandos.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Graduandos programas regulares. Permisos: registro y consulta.
39.	[S_SIAG_Adm] SIAG para Personal de Desarrollo.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Oficina de desarrollo. Permisos: registro, edición y consulta.
40.	[S_Task_Manager] Registro de actualizaciones de software personal TIC	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Personal gestión de recursos tecnológicos. Permisos: registro, edición y consulta.
41.	[S_SIAG_EGRESADOS] SIAG Administrativo Egresados	Administrativo-Admisiones	P.U. Desarrollo de Software. Contratista Egresados	Contratista egresados. Permisos: registro, edición y consulta.
42.	[S_SIAG_BA_I] SIAG Bienestar _ ICETEX	Casa Obando	P.U. Desarrollo de Software. Asesor Bienestar	Oficina de bienestar universitario.

				Permisos: consulta.
43.	[S_SIAG_BIBLIOTECA] SIAG Registro Multas de Biblioteca.	Bienestar Universitario	P.U. Desarrollo de Software. P.U. Biblioteca	Proceso de biblioteca. Permisos: registro, edición y consulta.
44.	[S_SGI] Sistema de Gestión Integrado	Egresados	P.U. Desarrollo de Software	Personal administrativo de planeación. Permisos: registro, edición y consulta.
45.	[S_Acciones] Sistema de Acciones y Mejoras	Docencia	P.U. Desarrollo de Software	Personal administrativo de planeación y control interno. Permisos: registro, edición y consulta.
46.	[S_HELPDESK] Sistema Inventario e Incidencias de Activos de TI	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Super_administrador Administrador Técnico Post_Only
47.	[S_Ponderados] Sistema de Ponderados UNIMAYOR	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Aspirantes a programas regulares IUCMC. Permisos: consulta.
48.	[S_PQR´S] Sistema Web de PQR´S	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Personal administrativo IUCMC. Permisos: registro, edición, consulta y borrado.

49.	[S_Directorio] Sistema Web Directorio Institucional	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Oficina TIC y comunicaciones. Permisos:
50.	[S_SIAG_ME] SIAG Modulo Externo de Egresados	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Contratista Egresados	Egresados IUCMC programas regulares. Permisos: registro, edición y consulta.
51.	[S_SIAG_MF] SIAG matricula Financiera Admisiones - Aspirantes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Admitidos programas regulares IUCMC. Permisos: registro y consulta.
52.	[S_SIAG_SNIES] SIAG Reporte a SNIES	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Auxiliar Vicerrectoría	Auxiliar administrativa vicerrectoría: permisos: consulta.
53.	[S_SIAG_Electoral] SIAG Elección Representantes Entes Institucionales	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Secretaria General	Secretaria general. Permisos: registro, edición y consulta.
54.	[S_SIAG_Bitácoras] SIAG reporte actividades Docentes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Docentes de programas regulares IUCMC. Permisos: registro, edición y consulta.
55.	[S_Utility] Sistema registro actividades Personal Desarrollo	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Personal oficina de desarrollo. Permisos:

				registro, edición y consulta.
56.	[S_SIAG_INV] SIAG Investigaciones	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Contratista Investigaciones	Proceso de investigaciones. Permisos: registro, edición y consulta.
57.	[S_R_FISICOS] SIAG Recursos Físicos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos	Personal gestión de recursos tecnológicos. Permisos: registro, edición y consulta.
58.	[S_SIAG_INT] SIAG Internacionalización	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos P.U. Internacionalización	Proceso de internacionalización. Permisos: registro, edición y consulta.
59.	[S_SIAG_LR] SIAG Liquidación Recaudos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Aux-Facultades	Personal administrativo IUCMC. Permisos: registro, edición y consulta.
60.	[S_SIRAEX_MFA] SIRAEX Matriculas Financieras Admisiones - Aspirantes	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Asesor Admisiones	Aspirantes a programas de inglés IUCMC. Permisos:
61.	[S_SIAG_PS] SIAG Proyección Social	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Proyección Social	Proceso de proyección social IUCMC. Permisos: registro, edición y consulta.
62.	[S_SIAG_BP] SIAG Banco de Proyectos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Asesor Planeación	Proceso de planeación y personal

				administrativo. Permisos: registro, edición y consulta.
63.	[S_SIRAEX_G] SIRAEX Graduandos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Contratista Egresados	Graduandos programas de inglés. Permisos: registro y consulta.
64.	[S_Consulta_F] Sistema Consulta Financiera	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Aux-Facultades	Oficina financiera IUCMC. Permisos: consulta.
65.	[S_Recursos_T] Sistema de Recursos Tecnológicos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos	Proceso de gestión de recursos tecnológicos. Permisos: registro, edición y consulta.
66.	[S_SIAG_Ambiental] Sistema Ambiental	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Contratista Ambiental	Contratista de ambiental. Permisos: registro, edición y consulta.
67.	[S_RESERVAS] Sistema de Reservas de Salas de Reunión	Gestión Recursos Tecnológicos	Contratista TIC	Administrador Usuario Normal
68.	[S_AGENDA] Sistema de Agenda Institucional	Gestión Recursos Tecnológicos	Contratista TIC	Administrador Usuario Normal
69.	[S_SAEVA]Sistema de Autoevaluación	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software	Administrador Usuario Normal
70.	[S_ENC] Sistema de Encuestas Unimayor	Gestión Recursos Tecnológicos	Contratista Desarrollo de Software	Administrador

71.	[S_SITH] Sistema de Talento Humano	Gestión y Desarrollo del Talento Humano	Gestión y Desarrollo del Talento Humano	Super_Usuario Administrador
72.	[S_UNICA] Sistema de Unidad de Correspondencia	Gestión Documental	Contratista Unidad de Correspondencia	Administrador Usuario Normal
73.	[S_ SICOF] Sistema Contable y Financiero	Gestión Financiera y Contable	Coordinadora Financiera	Administrador
74.	[S_SIABUC] Sistema de Automatización de Bibliotecas de la Universidad de Colima	Gestión de Biblioteca	Bibliotecóloga	Super_usuario Administrador Usuario nivel1 Usuario nivel2
75.	[S_CELESTE] Sistema Integrado Contable Financiero Enterprise.	Gestión Financiera y Contable	Gestión Financiera y Contable Gestión Recursos Tecnológicos	Oficina financiera IUCMC. Permisos: registro, edición y consulta.
[HW] EQUIPOS INFORMÁTICOS (Servidores, Hardware)				
76.	[SER_BCP_SIAG] Servidor Business Continuity Plan del SIAG	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
77.	[SER_SIAG] Servidor Sistema de Información Académica y Gestión	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	Personal administrativo con acceso a los diferentes módulos del SIAG
78.	[SER_WEB_BACKUPS] Servidor Sitios Web	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
79.	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
80.	[SER_ANTIVIRUS] Servidor Antivirus ESET y Máquinas Virtuales	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	

81.	[SER_SNIES] Servidor SNIES	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
82.	[SER_CAM_P] Servidor Cámaras IP, Pantallas Informativas y Aplicaciones WEB	Gestión Recursos tecnológicos	T.A. Red Datos y Servidores	
83.	[SER_SICOF] Servidor Sistema Financiero y Contable	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
84.	[SER_SIABUC_W] Servidor Consulta SIABUC Web	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
85.	[SER_MOODLE_DNS] Servidor Herramientas Virtuales de Aprendizaje	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
86.	[SER_SIABUC] Servidor SIABUC	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	Administrador
87.	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
88.	[HW_PC] Equipos de cómputo (escritorio y portátiles)	Todos	Todos	
89.	[HW_IMP] Impresoras	Administrativos - Docentes	Todos	
90.	[HW_ESC] Escáneres	Administrativos - Docentes	Todos	
91.	[HW_SWIT] Switch administrable	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
92.	[HW_FW] Firewall UTM	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
93.	[HW_WAP] Punto de Acceso Inalámbrico	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
94.	[HW_enrutadores] Enrutadores	Gestión Recursos Tecnológicos	Proveedor ISP	
95.	[HW_Radio_Enlace] Radio Enlace Interconexión Alterna	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores	
96.	[HW_Gateway] Gateway VoIP	Gestión Recursos Tecnológicos	proveedor ISP	

[COM] Redes de Comunicaciones				
97.	[COM_RT] Red Telefónica	Gestión Recursos Tecnológicos	Asesor TIC	
98.	[COM_Datos] Red de Datos	Gestión Recursos Tecnológicos	Asesor TIC	
99.	[COM_WIFI] Red inalámbrica	Gestión Recursos Tecnológicos	Asesor TIC	
100.	[COM_MAN] Red Área Metropolitana	Gestión Recursos Tecnológicos	Asesor TIC	
101.	[COM_ISP] Internet	Gestión Recursos Tecnológicos	Asesor TIC	
[SI] SOPORTES INFORMACIÓN				
102.	[SI_CD_ROM/DVD] Soportes de información en CD-ROOM y/o DVD	Todos	Todos	
103.	[SI_USB] Soportes de información en Discos Externos USB	Todos	Todos	
104.	[SI_IMPRESOS] Soportes de Información Impresos en Papel	Todos	Todos	
105.	[SI_NAS] Almacenamiento en la Red	Gestión Recursos Tecnológicos	Todos	
106.	[SI_AA] Almacenamiento de archivos en nube Privada	Gestión Recursos Tecnológicos	Todos	
107.	[SI_Drive] Almacenamiento en la Nube (Gmail)	Todos	Todos	
[AUX] EQUIPAMIENTO AUXILIAR				
108.	[AUX_UPS] Sistema de Alimentación Ininterrumpida	Gestión Recursos Tecnológicos	Asesor TIC	
109.	[AUX_AC]Aires Acondicionados	Gestión Recursos Tecnológicos	Asesor TIC	
110.	[AUX_Cabl_Elect] Cableado Eléctrico	Gestión Recursos Tecnológicos	Asesor TIC	

111.	[AUX_Cabl_Datos] Cableado Datos	Gestión Recursos Tecnológicos	Asesor TIC	
112.	[AUX_DEST] Equipo Destrucción de Papel	Gestión Documental	P.U. Archivo	
113.	[AUX_CF] Cajas Fuertes	Gestión Contable y Financiera	P.U. Presupuesto	
114.	[AUX_Tel] Teléfonos	Gestión Recursos Tecnológicos	Todos	
115.	[AUX_VIG] Cámaras de Vigilancia	Gestión Recursos Tecnológicos	Asesor TIC	
[L] INSTALACIONES				
116.	[L_Edificio] Edificios			
117.	[L_DATOS] Centros de Datos	Gestión Recursos Tecnológicos	Asesor TIC	
118.	[L_CANAL] Canalización (Cableados)	Gestión Recursos Tecnológicos	Asesor TIC	
119.	[L_GAB] Gabinete de red	Gestión Recursos Tecnológicos	Asesor TIC	
[P] PERSONAL				
120.	[P_UE] Usuarios Externos	Talento Humano	P.U. Talento Humano	
121.	[P_UI] Usuarios Internos	Talento Humano	P.U. Talento Humano	
122.	[P_ADM] Administradores de Sistemas	Gestión Recursos Tecnológicos	Desarrolladores	
123.	[P_DBA] Administrador de Bases de Datos	Gestión Recursos Tecnológicos	Desarrolladores	
124.	[P_SEC] Administradores de seguridad	Gestión Recursos Tecnológicos	Desarrolladores	
125.	[P_DES] Desarrollo Software	Gestión Recursos Tecnológicos	Desarrolladores	
126.	[P_CON] Contratistas	Talento Humano	P.U. Talento Humano	

127.	[Proveedores] Proveedores	Talento Humano	P.U. Talento Humano	
128.	[P_OCA] Ocasionales	Talento Humano	P.U. Talento Humano	

Tabla 2. Clasificación Activos de Información

6.2. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

Los riesgos asociados a seguridad y privacidad de la información junto con la valoración y el tratamiento se pueden visualizan en documento: "Matriz de Riesgos de Seguridad y Privacidad de la Información".

7. SEGUIMIENTO A CONTROLES DE RIESGOS

El seguimiento y monitoreo de controles de seguridad y privacidad de la información, se realiza para determinar el logro de los resultados esperados tomando como referencia lo dispuesto en el procedimiento "P2_ADMINISTRACION_DEL_RIESGO_V6" del subproceso Direccionamiento Estratégico publicado en el portal del Sistema de Gestión Integrado de la Institución Universitaria Colegio Mayor del Cauca.

8. PLAN DE CONTINUIDAD DEL NEGOCIO

El Sistema de Gestión de Seguridad de la información ha dispuesto el procedimiento para continuidad del negocio, cuyo objetivo es "Definir la forma como la Institución Universitaria Colegio Mayor del Cauca - IUCMC gestionará su infraestructura y servicios de TI para mantener la seguridad de la información en caso de un desastre o de otro incidente disruptivo". (Ver documento: 104.03.01.02.02.P.05 Procedimiento para continuidad del negocio).

9. POLÍTICAS DE SEGURIDAD 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.
Los objetivos de Seguridad de la Información son:

a. 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.
b. Atender y solucionar los incidentes de seguridad de la información reportados en la Institución Universitaria.
c. 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.

Esta política es revisada periódicamente por el Líder de Seguridad de la Información y la Alta Dirección, igualmente cuando se identifiquen cambios en los procesos y/o tecnología o se presente alguna condición que afecte la Seguridad de la información de la institución, esto como parte de lograr la mejora continua. En caso de realizarse cambios, la política será comunicada a las partes interesadas a través de los canales aprobados por la Alta Dirección de la institución.

10. PLAN DE CAPACITACIÓN

La institución Universitaria Colegio Mayor del Cauca ha definido el plan de capacitación y sensibilización de las políticas, normas y procedimientos de seguridad de la información, indicando medios y estrategias a utilizar, y mecanismos de evaluación de la interiorización de las actividades en el documento 04.03.01.02.02.D.09 Plan de Sensibilización de Seguridad de la Información.

11. MARCO LEGAL

Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

Decreto 1008 de 14 de Junio de 2018, lineamientos generales de la política de Gobierno Digital.

ISO 9001:2015; Norma de Sistemas de Gestión de Calidad (SGC),

NTC 5555:2011: norma técnica Colombiana para Sistema de Gestión de la Calidad en las Instituciones de Formación para el Trabajo (IFT).

NTC 5580:2011; norma técnica Colombiana para programas de formación para el trabajo en el área de idiomas.

ISO 14001; Norma de Sistemas de Gestión Ambiental (SGA), permite a las organizaciones demostrar su compromiso con el medio ambiente.

ISO 27000: Conjunto de estándares internacionales de Seguridad de la información.

12. BIBLIOGRAFÍA

Departamento Nacional De Planeación, Política Nacional de Seguridad Digital – CONPES 3854.

Documentos, Formatos y procedimientos SAIC, Institución Universitaria Colegio Mayor del Cauca. Disponible en http://10.20.30.2:8000/sgi/portada

GUIA 8 seguridad y privacidad de la información; MINTIC VERSION 3.0.1

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, corrupción y seguridad Digital. Versión 4. Departamento administrativo de la función pública (DAFP). Bogotá, Colombia Octubre 2018

NTC-ISO/IEC 27000:2014, Tecnología de la Información. Técnicas de Seguridad Sistemas de gestión de seguridad de información. Descripción y vocabulario.

13. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIO REALIZADO
2 de diciembre de 2019	Se realizó actualización de los activos de información.
26 de enero de 2021	Se realizó actualización de los activos de información.