PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaboró:	Revisó:	Aprobó:
Asesor (a) TIC	Asesor (a) TIC	Rector (a)

CONTENIDO

INDICE DE TABLAS

1. INTRODUCCIÓN

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].

EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado contra criterios de riesgos 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].

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. MARCO LEGAL

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.

6. 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, 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 planeación hasta la mejora continua.	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 tecnológica para el aseguramiento de la información institucional.	Daño en equipos o medios tecnológicos

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 gubernamental 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 los activos de información.	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 acceso a solo personal autorizado etc.)		Hurto de activos de información.

	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.		

7. PLAN DE ACCIÓN DE GESTION 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.

7.1. 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
	[S] SERVICIOS		
1	[S_SIAG] Servicios SIAG	Gestión Recursos Tecnológicos	T.U. Desarrollo de Software
2	[S_WEB]	Comunicaciones	Contratista Webmaster
3	[S_PROXY]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
4	[S_DHCP]		T.A. Red Datos y Servidores
5	[S_MAQUINAS_V]		T.A. Red Datos y Servidores
6	[S_ANTIVIRUS_ESET]		T.A. Red Datos y Servidores
7	[S_SNIES]	Fuera de uso	T.A. Red Datos y Servidores
8	[S_CAMARAS_IP]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
9	[S_SICOF]	Gestión Financiera y Contable	T.A. Red Datos y Servidores
10	[S_SIABUC_WEB]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
11	[S_SIABUC_LOCAL]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
12	[S_MOODLE]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
13	[S_DNS]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
14	[S_BACKUPS]	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores

	[D] DATOS/INFORMACIÓN	Gestión de Talento Humano	Contratista
15	[D_ADM] Datos Funcionarios	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos
16	[D_Vr_est] Datos estudiantes		
17	[BACKUPS] Copias de Seguridad	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
18	[INFO_R] Información restringida	Gestión Documental	P.U. Gestión Documental
19	[INFO_PUBLICA]	Gestión Documental	P.U. Gestión Documental

	[SW] APLICACIONES (Software)		
20	[SI_SICEED_Al]Sistema de Evaluación Docente -Alumnos	Gestión Recursos Tecnológicos	Red Datos y Servidores
21	[SI_ SICCED_De]Sistema de Evaluación Docente -Decano	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
22	[SI_ SICCED_Do]Sistema de Evaluación Docente - Docente	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
23	[SI_ SICCED_V]Sistema de Evaluación Docente -Vicerrector	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
24	[SI_SIAG]Sistema de Información y de Gestión [Administrativo]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
25	[SI_SIAG_ADM] SIAG Admin [Técnico Administrativo SIAG]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
26	[SI_SIAG_R] SIAG Reportes [Administrativo IUCMC]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
27	[SI_SIAG_V]Vicerrectoría Plantillas [SIAG Vicerr.]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
28	[SI_SIAG_P] SIAG Promedios MVC [Facultades]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
29	[SI_SIAG_ADM]SIAG Admisiones [Administrativo]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
30	[SI_SIAG_L] SIAG Liquidación [Recaudos - Certificados]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software

31	[SI_SIAG_L_M] SIAG Liquidación [Matriculas]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
32	[SI_SIAG_N] Consulta de Notas [SIAG]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
33	[SI_BIENESTAR]Bienestar Universitario	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
34	[SI_SIAG_B]SIAG Bienestar	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
35	[SI_SIRAEX_CONSULTA_N] Consulta de Notas Extensión - Arte Mayor	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
36	[SI_TASK MANAGER] Administrador de tareas [Adm Si - Adm Red]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
37	[SI_REG_LINEA_R] Registro En Línea [Regulares]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
38	[SI_REG_LINEA_E]Registro En Línea [Extensión]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
39	[SI_FACTURA_INSCIPCION_As] Factura Inscripción Unimayor [Aspirantes]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
40	[SI_SIRAEX_CONSULTA_REG_E]Consulta Registro Extensión	Administrativo-Admisiones	P.U. Desarrollo de Software
41	[SI_SIRAEX_ADM_CO]Académico Extensión [Administrativo Casa Obando]	Casa Obando	P.U. Desarrollo de Software
42	[SI_SIRAEX_ADM_BU] Académico Arte Mayor [Administrativo Bienestar U.]	Bienestar Universitario	P.U. Desarrollo de Software
43	[SI_SIRAEX_REG_N_Do]Registro de Notas Extensión [Docentes Inglés]	Docentes Ingles	P.U. Desarrollo de Software
44	[SI_SIAG_EGRESADOS] Registro Egresados	Egresados	P.U. Desarrollo de Software
45	[SI_SIAG_EGRESADOS_ADM] Egresados Administrador	Docencia	P.U. Desarrollo de Software
46	[SI_HELPDESK] Sistema Inventario e Incidencias de Activos de TI	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
47	[SI_OCS] Sistema Gestor de Inventario de activos TI	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
48	[SI_RESERVAS] Sistema de Reservas de Salas de Reunión	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software

49	[SI_AGENDA] Sistema de Agenda Institucional	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
50	[SI_SAEVA]Sistema de Autoevaluación	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
51	[SI_ENC] Sistema de Encuestas Unimayor	Gestión Recursos Tecnológicos	Contratista Desarrollo de Sw
52	[SI_DOC] Sistema Documentos IUCMC	Gestión Recursos Tecnológicos	Contratista Desarrollo de Sw
53	[SI_SITH] Sistema de Talento Humano	Talento Humano	Talento Humano
54	[SI_UNICA] Sistema de Unidad de Correspondencia	Gestión Documental	Contratista UC
55	[SI_SALUD_OCU] Sistema Ausentismo Laboral -Salud Ocupacional	Salud Ocupacional	Contratista SO
56	[SI_ SICOF] Sistema Contable y Financiero	Gestión Financiera y Contable	Coordinadora Financiera
57	[SI_SIABUC] Sistema de Automatización de Bibliotecas de la Universidad de Colima	Gestión de Biblioteca	Bibliotecóloga

	[HW] EQUIPOS INFORMATICOS (Hardware)		
58	[SER_BCP_SIAG] Servidor Business Continuity Plan del SIAG	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
59	[SER_SIAG] Servidor Sistema de Información Académica y Gestión	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
60	[SER_WEB_PROXY_BACKUPS] Servidor Sitios Web	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
61	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
62	[SER_ANTIVIRUS] Servidor Antivirus ESET y Máquinas Virtuales	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
63	[SER_SNIES] Servidor SNIES	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
64	[SER_CAM_IP] Servidor Cámaras IP y Aplicaciones WEB	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores

65	[SER_SICOF] Servidor Sistema Financiero y Contable	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
66	[SER_SIABUC WEB_ITS] Servidor Consulta SIABUC Web y Servicios de Tecnología de la Información.	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
67	[SER_MOODLE_ DNS] Servidor Herramientas Virtuales de Aprendizaje	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
68	[SER_SIABUC] Servidor SIABUC	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
69	[SER_DHCP- PROXY] Servidor DHCP y Proxy alterno.	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
70	[HW_PC] Equipos de cómputo (escritorio y portátiles)	Todos	Todos
71	[HW_IMP] Impresoras	Administrativos - Docentes	Todos
72	[HW_ESC] Escáneres	Administrativos - Docentes	Todos
73	[HW_SWIT] Switch administrable	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
74	[HW_FW] Firewall UTM	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
75	[HW_WAP] Punto de Acceso Inalámbrico	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
76	[HW_PBX] Central Telefónica	Gestión Recursos Tecnológicos	proveedor

	[COM] Redes de Comunicaciones		
77	[COM_RT] Red Telefónica	Gestión Recursos Tecnológicos	Asesor TIC
78	[COM_Datos] Red de Datos	Gestión Recursos Tecnológicos	Asesor TIC
79	[COM_WIFI] Red inalámbrica	Gestión Recursos Tecnológicos	Asesor TIC
80	[COM_LAN] Red Local	Gestión Recursos Tecnológicos	Asesor TIC

81	[COM_ISP] Internet	Gestión Recursos Tecnológicos	Asesor TIC

	[SI] Soportes Información		
82	[SI_CD_ROM/DVD] Soportes de información en CD-ROOM y/o DVD	Todos	Todos
83	[SI_USB] Soportes de información en Discos Externos USB	Todos	Todos
84	[SI_IMPRESOS] Soportes de Información Impresos en Papel	Todos	Todos
85	[SI_SAN] Almacenamiento en Red Almacenamiento en la Nube	Gestión Recursos Tecnológicos	Todos

86	**[AUX] Equipamiento auxiliar**		
87	[AUX_UPS] Sistema de Alimentación Ininterrumpida	Gestión Recursos Tecnológicos	Asesor TIC
88	[AUX_AC]Aires Acondicionados	Gestión Recursos Tecnológicos	Asesor TIC
89	[AUX_Cabl_Elect] Cableado Eléctrico	Gestión Recursos Tecnológicos	Asesor TIC
90	[AUX_Cabl_Datos] Cableado Datos	Gestión Recursos Tecnológicos	Asesor TIC
91	[AUX_DEST] Equipo Destrucción de Papel	Gestión Documental	P.U.Archivo
92	[AUX_CF] Cajas Fuertes	Gestión Contable y Financiera	P.U. Presupuesto
93	[AUX_VIG] Cámaras de Vigilancia	Gestión Recursos Tecnológicos	Asesor TIC

	[L] Instalaciones		
94	[L_Edificio] Edificios		
95	[L_DATOS] Centros de Datos	Gestión Recursos Tecnológicos	Asesor TIC
96	[L_CANAL] Canalización (Cableados)	Gestión Recursos Tecnológicos	Asesor TIC

97	[L_GAB] Gabinete de red	Gestión Recursos Tecnológicos	Asesor TIC

	[P] Personal		
98	[P_UE] Usuarios Externos	Talento Humano	P.U. Talento Humano
99	[P_UI] Usuarios Internos	Talento Humano	P.U. Talento Humano
100	[P_ADM] Administradores de Sistemas	Gestión Recursos Tecnológicos	Desarrolladores
101	[P_DBA] Administrador de Bases de Datos	Gestión Recursos Tecnológicos	Desarrolladores
102	[P_SEC] Administradores de seguridad	Gestión Recursos Tecnológicos	Desarrolladores
103	[P_DES] Desarrollo Software	Gestión Recursos Tecnológicos	Desarrolladores
104	[P_CON] Contratistas	Talento Humano	P.U. Talento Humano
105	[Proveedores]	Talento Humano	P.U. Talento Humano
106	[P_OCA] Ocasionales	Talento Humano	P.U. Talento Humano

Tabla 1. Clasificación Activos de Información

7.2. IDENTIFICACION 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 anexo1: "Matriz de Riesgos de Seguridad y Privacidad de la Información".

8. SEGUIMIENTO A CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El seguimiento y monitoreo de controles, se realiza para determinar el logro de los resultados esperados y se toma como referencia lo dispuesto en el procedimiento "P2_ADMINISTRACION_DEL_RIESGO_V6" del subproceso Direccionamiento Estratégico

publicado en el portal del Sistema de Aseguramiento Interno de la Calidad de la Institución Universitaria Colegio Mayor del Cauca.

9. 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 gestionara su infraestructura y servicios de TI para mantener la seguridad de la información en caso de un desastre o de otro incidente disruptivo". (Ver anexo2: 104.03.01.02.02.P.05 Procedimiento para continuidad del negocio).

10. POLÍTICAS DE SEGURIDAD DE LA INFORMACION

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.

11. 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.

12. 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.

13. ACCIONES DE TRATAMIENTO PARA LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Ver Plan de tratamiento de Riesgos (PTR) del documento anexo1: "Matriz de Riesgos de Seguridad y Privacidad de la Información".

14. 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.

15. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIOS REALIZADOS