PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

V.3

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

CONTENIDO

1. INTRODUCCIÓN

La Institución Universitaria Colegio Mayor del Cauca consciente de la importancia de asegurar la información, debe generar un marco normativo soportado en los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) emitido por MINTIC, el componente transversal de la estrategia Gobierno Digital y la norma ISO/IEC 27001:2013 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 Subproceso 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.

4.2 ESPECÍFICOS

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

5. TÉRMINOS Y DEFINICIONES

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

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

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 - 100.01.01.01.P.02 – SGI 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 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.

[1] Modelo de Seguridad y Privacidad de la Información _ MINTIC. https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

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.

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

6.1 FASE DE DIAGNOSTICO DEL MSPI

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

Figura 2. Fase de Diagnostico

DIAGNOSTICO			
METAS	Actividades/Instrumentos	TIEMPO ESTIMADO	RESULTADOS
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Institución Universitaria	Diligenciamiento del Instrumento Evaluación MSPI emitido por MINTIC.	01/02/2019 - 14/04/2019	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.	14/04/2019 - 30/12/2019	Declaración de Aplicabilidad. Riesgos actualizados

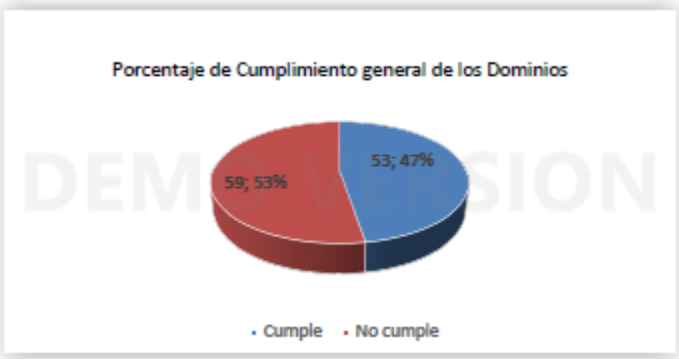
Para desarrollar la fase de diagnóstico la Institución Universitaria Colegio Mayor del Cauca realizo en la vigencia 2019 las tareas programadas y descritas en la anterior tabla, además ejecuto la auditoria interna de seguridad y privacidad de la información haciendo uso de la herramienta MSPI (Modelo 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 y la auditoria permite conocer el estado actual se seguridad y privacidad de la información en la Institución Universitaria Colegio Mayor del Cauca.

EFECTIVIDAD DE CONTROLES

La Institución Universitaria realizo una auditoria interna para cumplir con el objetivo:" Evaluar el cumplimiento de los controles del estándar ISO/IEC 27001:2013 en los diferentes procesos de la Institución Universitaria Colegio Mayor del Cauca", obteniendo el 47% de implementación de los controles y un 53% de controles que requieren de acciones de mejoras.



Fuente: Informe auditoria interna 2019

6.1.2 BRECHA ANEXO A - ISO 27001:2013

La brecha encontrada, se puede apreciar en la siguiente tabla, evidenciando el porcentaje de cumplimiento de cada dominio de la norma ISO/IEC 27001:2013

DOMINIO	CUMPLE	NO CUMPLE
5	100 %	0%
6	33 %	67 %
7	17 %	83 %
8	60 %	40 %
9	50 %	50 %

10	50%	50 %
11	36 %	64 %
12	50 %	50 %
13	57 %	43 %
14	54 %	46 %
15	40 %	60 %
16	29 %	71 %
17	75 %	25 %
18	50 %	50 %

6.2 FASE DE PLANEACIÓN

Para desarrollar esta fase la Institución Universitaria toma como punto de partida los resultados obtenidos en la fase anterior para 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.

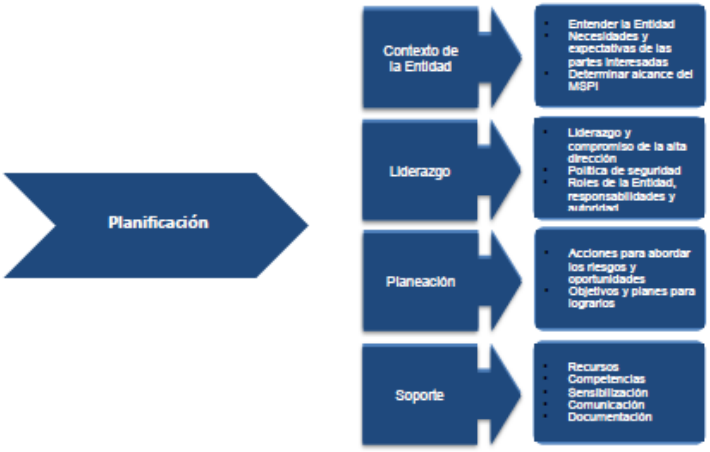


Figura 3. Fase de planificación[2]

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

6.2.1 PLAN DE SEGURIDAD DE LA INFORMACIÓN

No.	ACTIVIDAD	FECHA DE INICIO	FECHA DE FIN	PRODUCTO DE LA ACTIVIDAD
1	Realizar y socializar informe auditoria interna de seguridad y privacidad de la información 2019.	8-ene-20	10-ene-20	Documento Informe de auditorio 2019. Acta de socialización
2	Apoyo en la implementación de acciones de Seguridad y Privacidad de la información como requisitos de resultado de la auditoria de seguridad y privacidad de la información vigencia 2019.	10-feb-20	30-jun-20	Registro Mejoras de Seguridad y Privacidad de la información en Aplicativo
3	Actualizar la Matriz MSPI propuesta por Min TIC "Instrumento de identificación de la línea base de seguridad administrativa y técnica". (Cumplimiento política de Gobierno Digital y ley de transparencia).	10-feb-20	30-jun-20	Matriz MSPI actualizada.
4	Revisar, actualizar, registrar y realizar primer seguimiento de riesgos de seguridad y privacidad de la información en el aplicativo Institucional	14-ene-19	30-jun-20	Registro de riesgos de seguridad y privacidad de la información en aplicativo.

5	Revisar y actualizar de la declaración de aplicabilidad.	4-may-20	30-jun-20	Documento Declaración de aplicabilidad actualizada.
6	Generar las siguientes políticas de seguridad y privacidad de la información: . Controles criptográficos . Dispositivos Móviles . Escritorio Limpio y pantalla limpia. . Intercambio de Información (Digital y física)	3-ago-20	14-dic-20	Documentos con cada política.
7	Generar los siguientes Procedimientos o Documentos: . Copias de Respaldo . Sistema de Video vigilancia. . Gestión de medios removibles. . Áreas seguras (Documento)	3-ago-20	14-dic-20	Documentos de procedimientos.
8	Gestión de indicadores de Seguridad y Privacidad de la Información	3-mar-20	14-dic-20	Documento con indicadores.
9	Revisar y/o actualizar los documentos de seguridad y privacidad de la información que reposan en el sitio interno SGI (http://10.20.30.2:8000/sgi/subproceso/categorias/18)	3-ago-20	14-dic-20	Documentos actualizados.
	Realizar Supervisión puesto de trabajo relacionado con : . Ubicación equipo de cómputo. . Estado cableado de datos y eléctrico . Inicio seguro de sesión (contraseña de ingreso PC)	16-mar-20	31-mar-20	Lista de chequeo. Informe.
10	. Bloqueo de pantalla después de 15 min de inactividad . Puertas y ventanas.	15-sep-20	30-sep-20	
11	Apoyo auditoria de seguridad y privacidad de la información.	3-ago-20	14-dic-20	Plan de auditoria

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 104.03.01.02.02.D.08 Roles Y Responsabilidades Seguridad De La Información, disponible en el link http://10.20.30.2:8000/sgi/documentos/D8-_ROLES_Y_RESONSABILIDADES_V1.pdf, 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
- ✓ Asesor TIC
- ✓ 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_SIAG] Servicios SIAG	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
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_V]		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 Academico – Administrativo	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
22.	[S_ SICCED_DA]Sistema de Evaluación Docente – Alumnos	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
23.	[S_ SICCED_DD]Sistema de Evaluación Docente – Decano	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
24.	[S_ SICCED_V]Sistema de Evaluación Docente -Vicerrector	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
25.	[S_SIAG_R] SIAG Reporte [Administrativos]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
26.	[S_SIAG_P] SIAG Promedio MVC – Facultades	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
27.	[S_SIAG_ BU] SIAG Bienestar Universitario	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
28.	[S_SIAG_RN_PR] SIAG Registro de Notas programas Regulares	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
29.	[S_SIAG_CN-PR] SIAG Consulta de Notas Programas Regulares.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
30.	[S_SIAG_RL_PR]SIAG Registro en Línea Programas Regulares	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
31.	[S_SIAG_L] SIAG Liquidación [Recaudos - Certificados]	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
32.	[S_SIRAEX_RL] Sistema de Información Académico Extensión Registro en Línea.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
33.	[S_SIRAEX_AA] SIRAEX Admisiones para Administrativos de Admisiones	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software. Asesor Admisiones.
34.	[S_FACTURA_I] Factura de Inscripción Aspirantes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
35.	[S_SIRAEX_AC]SIRAEX Académico para administrativos Ingles.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
36.	[S_SIRAEX_RN] SIRAEX Registro Notas Ingles	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software

37.	[S_SIRAEX_CN] SIRAEX Consulta de Notas	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
38.	[S_SIAG_G] SIAG Registro Graduandos.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
39.	[S_SIAG_Adm] SIAG para Personal de Desarrollo.	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
40.	[S_Task_Manager] Registro de actualizaciones de software personal TIC	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
41.	[S_SIAG_EGRESADOS] SIAG Administrativo Egresados	Administrativo-Admisiones	P.U. Desarrollo de Software. Contratista Egresados
42.	[S_SIAG_BA_I] SIAG Bienestar _ ICETEX	Casa Obando	P.U. Desarrollo de Software. Asesor Bienestar
43.	[S_SIAG_BIBLIOTECA] SIAG Registro Multas de Biblioteca.	Bienestar Universitario	P.U. Desarrollo de Software. P.U. Biblioteca
44.	[S_SIRAEX_REG_N_D] Registro de Notas Extensión [Docentes Inglés]	Docentes Ingles	P.U. Desarrollo de Software
45.	[S_SGI] Sistema de Gestión Integrado	Egresados	P.U. Desarrollo de Software
46.	[S_Acciones] Sistena de Acciones y Mejoras	Docencia	P.U. Desarrollo de Software
47.	[S_HELPDESK] Sistema Inventario e Incidencias de Activos de TI	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
48.	[S_Ponderados] Sistema de Ponderados UNIMAYOR	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
49.	[S_PQR´S] Sistema Web de PQR´S	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
50.	[S_Directorio] Sistema Web Directorio Institucional	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
51.	[S_SIAG_ME] SIAG Modulo Externo de Egresados	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Contratista Egresados
52.	[S_SIAG_MF] SIAG matricula Financiera Admisiones - Aspirantes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
53.	[S_SIAG_SNIES] SIAG Reporte a SNIES	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Auxiliar Vicerrectoria
54.	[S_SIAG_Electoral] SIAG Elección Representantes Entes Institucionales	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Secretaria General

55.	[S_SIAG_Bitácoras] SIAG reporte actividades Docentes	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
56.	[S_Utility] Sistema registro actividades Personal Desarrollo	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software
57.	[S_SIAG_INV] SIAG Investigaciones	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software Contratista Investigaciones
58.	[S_R_FISICOS] SIAG Recursos Físicos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos
59.	[S_SIAG_INT] SIAG Internacionalización	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos P.U. Internacionalización
60.	[S_SIAG_LR] SIAG Liquidación Recaudos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Aux-Facultades
61.	[S_SIRAEX_MFA] SIRAEX Matriculas Financieras Admisiones - Aspirantes	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Asesor Admisiones
62.	[S_SIAG_PS] SIAG Proyección Social	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Proyección Social
63.	[S_SIAG_BP] SIAG Banco de Proyectos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Asesor Planeación
64.	[S_SIRAEX_G] SIRAEX Graduandos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Contratista Egresados
65.	[S_Consulta_F] Sistema Consulta Financiera	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Aux-Facultades
66.	[S_Recursos_T] Sistema de Recursos Tecnológicos	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos
67.	[S_SIAG_Ambiental] Sistema Ambiental	Gestión Recursos Tecnológicos	Gestión Recursos Tecnológicos Contratista Ambiental
68.	[S_RESERVAS] Sistema de Reservas de Salas de Reunión	Gestión Recursos Tecnológicos	Contratista TIC
69.	[S_AGENDA] Sistema de Agenda Institucional	Gestión Recursos Tecnológicos	Contratista TIC
70.	[S_SAEVA]Sistema de Autoevaluación	Gestión Recursos Tecnológicos	P.U. Desarrollo de Software

71.	[S_ENC] Sistema de Encuestas Unimayor	Gestión Recursos Tecnológicos	Contratista Desarrollo de Software
72.	[S_SITH] Sistema de Talento Humano	Gestión y Desarrollo del Talento Humano	Gestión y Desarrollo del Talento Humano
73.	[S_UNICA] Sistema de Unidad de Correspondencia	Gestión Documental	Contratista Unidad de Correspondencia
74.	[S_ SICOF] Sistema Contable y Financiero	Gestión Financiera y Contable	Coordinadora Financiera
75.	[S_SIABUC] Sistema de Automatización de Bibliotecas de la Universidad de Colima	Gestión de Biblioteca	Bibliotecóloga
76.	[S_CELESTE] Sistema Integrado Contable Financiero Enterprise.	Gestión Financiera y Contable	Gestión Financiera y Contable Gestión Recursos Tecnológicos
[HW] EQUIPOS INFORMÁTICOS (Servidores, Hardware)			
77.	[SER_BCP_SIAG] Servidor Business Continuity Plan del SIAG	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
78.	[SER_SIAG] Servidor Sistema de Información Académica y Gestión	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
79.	[SER_WEB_BACKUPS] Servidor Sitios Web	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
80.	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
81.	[SER_ANTIVIRUS] Servidor Antivirus ESET y Máquinas Virtuales	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
82.	[SER_SNIES] Servidor SNIES	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
83.	[SER_CAM_P] Servidor Cámaras IP, Pantallas Informativas y Aplicaciones WEB	Gestión Recursos tecnológicos	T.A. Red Datos y Servidores
84.	[SER_SICOF] Servidor Sistema Financiero y Contable	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
85.	[SER_SIABUC_W] Servidor Consulta SIABUC Web	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
86.	[SER_MOODLE_DNS] Servidor Herramientas Virtuales de Aprendizaje	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores

87.	[SER_SIABUC] Servidor SIABUC	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
88.	[SER_DHCP] Servidor DHCP	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
89.	[HW_PC] Equipos de cómputo (escritorio y portátiles)	Todos	Todos
90.	[HW_IMP] Impresoras	Administrativos - Docentes	Todos
91.	[HW_ESC] Escáneres	Administrativos - Docentes	Todos
92.	[HW_SWIT] Switch administrable	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
93.	[HW_FW] Firewall UTM	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
94.	[HW_WAP] Punto de Acceso Inalámbrico	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
95.	[HW_enrutadores] Enrutadores	Gestión Recursos Tecnológicos	Proveedor ISP
96.	[HW_Radio_Enlace] Radio Enlace Interconexión Alterna	Gestión Recursos Tecnológicos	T.A. Red Datos y Servidores
97.	[HW_Gateway] Gateway VoIP	Gestión Recursos Tecnológicos	proveedor ISP
[COM] Redes de Comunicaciones			
98.	[COM_RT] Red Telefónica	Gestión Recursos Tecnológicos	Asesor TIC
99.	[COM_Datos] Red de Datos	Gestión Recursos Tecnológicos	Asesor TIC
100	[COM_WIFI] Red inalámbrica	Gestión Recursos Tecnológicos	Asesor TIC
101	[COM_MAN] Red Area Metropolitana	Gestión Recursos Tecnológicos	Asesor TIC
102	[COM_ISP] Internet	Gestión Recursos Tecnológicos	Asesor TIC
[SI] SOPORTES INFORMACIÓN			
103	[SI_CD_ROM/DVD] Soportes de información en CD-ROOM y/o DVD	Todos	Todos
104	[SI_USB] Soportes de información en Discos Externos USB	Todos	Todos
105	[SI_IMPRESOS] Soportes de Información Impresos en Papel	Todos	Todos

106	[SI_NAS] Almacenamiento en la Red	Gestión Recursos Tecnológicos	Todos
107	[SI_AA] Almacenamiento de archivos en nube Privada	Gestión Recursos Tecnológicos	Todos
108	[SI_Drive] Almacenamiento en la Nube (Gmail)	Todos	Todos
[AUX] EQUIPAMIENTO AUXILIAR			
109	[AUX_UPS] Sistema de Alimentación Ininterrumpida	Gestión Recursos Tecnológicos	Asesor TIC
110	[AUX_AC]Aires Acondicionados	Gestión Recursos Tecnológicos	Asesor TIC
111	[AUX_Cabl_Elect] Cableado Eléctrico	Gestión Recursos Tecnológicos	Asesor TIC
112	[AUX_Cabl_Datos] Cableado Datos	Gestión Recursos Tecnológicos	Asesor TIC
113	[AUX_DEST] Equipo Destrucción de Papel	Gestión Documental	P.U. Archivo
114	[AUX_CF] Cajas Fuertes	Gestión Contable y Financiera	P.U. Presupuesto
115	[AUX_Tel] Teléfonos	Gestión Recursos Tecnológicos	Todos
116	[AUX_VIG] Cámaras de Vigilancia	Gestión Recursos Tecnológicos	Asesor TIC
[L] INSTALACIONES			
117	[L_Edificio] Edificios		
118	[L_DATOS] Centros de Datos	Gestión Recursos Tecnológicos	Asesor TIC
119	[L_CANAL] Canalización (Cableados)	Gestión Recursos Tecnológicos	Asesor TIC
120	[L_GAB] Gabinete de red	Gestión Recursos Tecnológicos	Asesor TIC
[P] PERSONAL			
121	[P_UE] Usuarios Externos	Talento Humano	P.U. Talento Humano
122	[P_UI] Usuarios Internos	Talento Humano	P.U. Talento Humano
123	[P_ADM] Administradores de Sistemas	Gestión Recursos Tecnológicos	Desarrolladores
124	[P_DBA] Administrador de Bases de Datos	Gestión Recursos Tecnológicos	Desarrolladores
125	[P_SEC] Administradores de seguridad	Gestión Recursos Tecnológicos	Desarrolladores

126	[P_DES] Desarrollo Software	Gestión Recursos Tecnológicos	Desarrolladores
127	[P_CON] Contratistas	Talento Humano	P.U. Talento Humano
128	[Proveedores] Proveedores	Talento Humano	P.U. Talento Humano
129	[P_OCA] Ocasionales	Talento Humano	P.U. Talento Humano

6.2.6 INTERACIÓN MSPI CON EL SISTEMA DE GESTIÓN DOCUMENTAL

Para la vigencia 2020 se debe evaluar y actualizar el Instrumento MSPI para evaluar la efectividad de la etapa de planeación y cumplimientos legales.

6.2.7 IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGO

El proceso de identificación, valoración y tratamiento de riesgos se encuentra detallado en el documento 104.01.02.02.D.16 Plan de Tratamiento de Riesgos de seguridad y privacidad de la información disponible en: https://unimayor.edu.co/web/18-unimayor/planeacion/2856-plan-de-tratamiento-de-riesgos-de-seguridad-y-privacidad-de-la-informacion#ano-2019; 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 104.03.01.02.02.D.09 Plan de sensibilización seguridad de la información, disponible en: http://10.20.30.2:8000/sgi/documentos/D9-_PLAN_DE_SENSIBILIZACI%C3%93N_SEG._DE_LA_INFORMACI%C3%93N_V1.pdf; aplicable en todos los niveles de la entidad (Directivos, funcionarios, academia y terceros)

6.3 FASE DE IMPLEMENTACIÓN

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

Figura 4. Fase de implementación

6.3.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La IUCMC debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos 2019, 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 300.07.01.01.02.P.01 control de documentos.

6.3.2 IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO

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

6.3.3 INDICADORES DE GESTIÓN

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

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

La Institución Universitaria ha generado los indicadores de gestión de seguridad y privacidad de la información en el documento Formulación y control de indicadores de seguridad de la

información, siguiendo la guía N°. 9 (Indicadores de gestión de seguridad y privacidad de la información) de MINTIC.

Proceso	Nombre	Objetivo del indicador	Fórmula	Meta	Periodicidad de medición	Responsable de cumplir la meta
Gestión recursos tecnológicos	Incidentes de seguridad de la información (físicos, lógicos, electrónicos)	Monitorear y Reducir el número de incidentes de seguridad de la información	(#Incidentes de seguridad de la información atendidos efectiva y oportunamente/ #total de incidentes reportados) *100	80%	trimestral	Líder de Seguridad de la información
Gestión y Desarrollo del Talento Humano	Usuarios activos e inactivos	Mantener actualizado los usuarios de los sistemas de información	(# usuarios vigentes o activos en el directorio activo / [Total de personas vigentes en talento humano) * 100	90%	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	asesor TIC
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

Fuente: documento 104.01.02.02.D.18 SGI – Institución Universitaria Colegio Mayor del Cauca.

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 grafica

Figura 5. Fase de Evaluación y Desempeño

6.4.1 PLAN DE REVISIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DE MSPI

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

ACTIVIDAD	PERIODICIDAD DE EJECUCION
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 veces 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.	Trimestralmente
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 500.01.03.01.P.03 PROCEDIMIENTO AUDITORÍAS INTERNAS, disponible en: http://10.20.30.2:8000/sgi/documentos/P3-_AUDITORIAS_INTERNAS_V9.pdf, debe adicionar dentro del plan de auditorías la revisión del Sistema de Gestión de Seguridad y Privacidad de la información y los controles implementados a través del MSPI.

6.5 FASE DE MEJORA CONTINUA

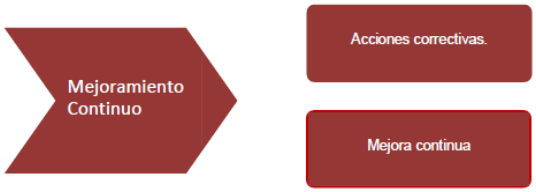


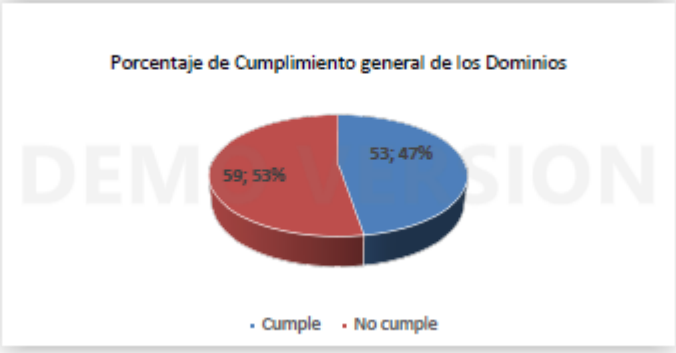
Figura 6. Fase de Mejora Continua.

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

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 300.07.01.01.02.P.03 ACCIONES CORRECTIVAS, PLANES DE MEJORAMIENTOY SALIDAS NO CONFORMES (http://10.20.30.2:8000/sgi/documentos/P3-_ACCIONES_V8.pdf)

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 identificó valorando el cumplimiento de controles de la ISO/IEC 27001: 2013 mediante la ejecución de auditoria interna realizada en Diciembre 2019.
Obteniendo un avance del 47% de controles implementados, por lo tanto se debe implementar y/o generar acciones de mejora a un 53 % de los controles, como se muestra en la siguiente gráfica.



8. ADOPCIÓN DEL PROTOCOLO IPV6

8.1 FASE DE PLANEACIÓN

Entre el año 2015 y 2016 se documenta 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 realizará 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
Volp 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 año 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.

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:

CONPES 3854 DE 2016 por el cual se establece la política nacional de seguridad digital en la república de Colombia.
DECRERO 612 DE 2018 por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.

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).

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

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 1273 DE 2009 por medio del cual se modifica el código penal, crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones "TIC", entre otras disposiciones.

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.

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.

LEY 527 DE 2009 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

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.

104.03.01.02.02.P.05 Procedimiento Para Continuidad Del Negocio.

104.03.01.02.02. R.21formato Declaración De Aplicabilidad

104.03.01.02.02.P.04 Gestión De Incidentes De Seguridad De La Información.

104.01.02.02.D.03 política, alcance y objetivos de seguridad de la información.

104.03.01.02.02.D.08 Roles Y Responsabilidades Seguridad De La Información.

104.03.01.02.02.D.09 Plan De Sensibilización Seguridad De La Información

104.03.01.02.02.D.10 Política De Seguridad De La Información Control De Acceso.

104.03.01.02.02.D.11 Política De Seguridad De La Información Desarrollo Seguro.

104.03.01.02.02.D.12 Política De Seguridad De La Información Gestión De Los Activos De Información.

104.03.01.02.02.D.13 Política De Seguridad Para Proveedores.

104.01.02.02.D.15 Plan De Seguridad Y Privacidad De La Información.

104.01.02.02.D.16 Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información.

Formato Evento O Incidente De Seguridad De La Información.

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

200.09.04.03.04.P.04 Formación Y Capacitación Del Personal

300.07.01.01.02.P.03 Acciones Correctivas, Planes De Mejoramiento y Salidas No Conformes.

300.07.01.01.02.P.01 Control De Documentos.

500.01.03.01.P.03 Procedimiento Auditorías Internas.

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.
28/ 01/2020	Revisión general y actualización del documento de acuerdo a resultados obtenido de la auditoria interna de seguridad y privacidad de la información vigencia 2019.