Universidad de la Amazonia

Universidad de la Amazonia

Plan de Seguridad y Privacidad de la Información

2026

TABLA DE CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

1 INTRODUCCIÓN

La seguridad y privacidad de la información es un aspecto relevante para las organizaciones, pues mantiene un equilibrio en los tres pilares fundamentales mencionados en la norma ISO 27001:2013, los cuales son: Disponibilidad, Integridad y Confiablidad. A su vez, la implementación del ciclo PHVA en los procesos misionales es una estrategia de evaluación primordial para conocer el estado actual de la seguridad y privacidad de la información, procedimientos, políticas y talento humano relacionado, para garantizar que la información, como activo esencial de cualquier empresa, se encuentre protegido frente a incidentes que a diario vulneran cada una de estas características. Del mismo modo, es necesario identificar y contrarrestar los riesgos informáticos, teniendo en cuenta el auge de las Tecnologías de la Información (TICs), porque constantemente avanzan en la degradación de los servicios tecnológicos de las organizaciones. De esta manera, existen metodologías de riesgos informáticos como MAGERIT, NSIT, CRAMM, OCTAVE, ISO 27005:2018, entre otras, que establecen controles para mantener el equilibrio entre los pilares de seguridad de la información.

Por lo anterior, es primordial definir e implementar estrategias, políticas, procedimientos, controles, etc., de seguridad y privacidad de la información, para disminuir la probabilidad de ocurrencia de amenazas y ataques informáticos y mejorar la productividad de los procesos asociados.

Así, la Universidad de la Amazonia, en relación con el Sistema Integrado de Gestión de Calidad, el Acuerdo 017 de 2017 “Por el cual se adoptan las políticas del Oficina de Asesora de Tecnologías de la Información de la Universidad de la Amazonia”, el Modelo de Seguridad de la Información (MSPI), alineado con el Marco de Referencia de Arquitectura TI y otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión, realiza la elaboración del presente plan de Seguridad y Privacidad de la Información para dar cumplimiento a

los requerimientos exigidos por el Ministerio de Educación Nacional, en la Ley 1474 de 2011, el Modelo Integrado de Planeación y Gestión - MIPG, el Decreto 103 de 2015, y la Resolución 3564 de 2015 y Ley 2013 del 30 de diciembre de 2019.

El presente plan pretende evaluar, anualmente, el estado actual de la gestión realizada por la Oficina Asesora de Tecnologías de la Información (OATI) en la definición, ejecución y retroalimentación de los procedimientos, políticas, actividades, y demás aspectos, relacionados con la seguridad y privacidad de la información.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Definir el plan de seguridad y privacidad de la información de la Universidad de la Amazonia para garantizar la disponibilidad, integridad y confiablidad de la información institucional.

2.2 OBJETIVOS ESPECÍFICOS

- Ejecutar el instrumento de evaluación MSPI establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

- Identificar el cumplimiento del Acuerdo No. 017 de 2017 “Por el cual se adoptan las políticas del Oficina Asesora de Tecnologías de la Información de la Universidad de la Amazonia” por parte de las partes interesadas internas y externas.

- Identificar el nivel de madurez de los controles de seguridad de la información establecidos en el Acuerdo No. 017 de 2017 “Por el cual se adoptan las políticas del Oficina Asesora de Tecnologías de la Información de la Universidad de la Amazonia”.

3 ALCANCE DEL DOCUMENTO

De acuerdo con las actividades a realizar dentro del plan de seguridad y privacidad de la información, el alcance de este documento corresponde a:

- Definición del cronograma de actividades para aplicación, evaluación y retroalimentación de los procedimientos, políticas, controles, estrategias y buenas prácticas de seguridad de la información.

- Asignación de responsabilidades a todos los funcionarios administrativos de la Universidad de la Amazonia.

4 GLOSARIO DE TÉRMINOS

- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización[1].

- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal[1].

- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000) [1].

- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000) [1].

- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoria[1].

- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

[1] ISO/IEC 27000 - Vocabulario estándar para el SGSI.

- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma[1].

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias[1].

- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información[1].

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas[1].

- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- Modelo de Seguridad y Privacidad de la Información (MSPI): Documento que conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos[2].

[2] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5 RESPONSABILIDAD

5.1 OFICINA ASESORA DE TECNOLOGÍAS DE LA INFORMACIÓN

Proporcionar soluciones a los servicios TI y brindar la gestión necesaria desde el punto de vista de las TIC, a las áreas que lo requieran mediante altos niveles de seguridad, confiabilidad y confidencialidad, garantizando la continuidad de la prestación de los servicios institucionales para contribuir al cumplimiento de la misión institucional.

5.2 FUNCIONARIOS ADMINISTRATIVOS

Es responsabilidad de cada usuario la adopción de la política de seguridad de la información establecida en el Acuerdo No. 017 de 2017.

6 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la elaboración del plan de seguridad y privacidad de la información de la Universidad de la Amazonia, se utilizó el ciclo de operación del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el MinTIC (ver Figura 1).

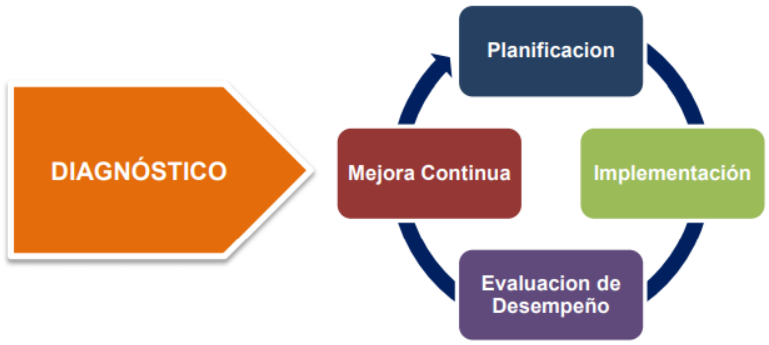

Figura 1. Fases del ciclo de operación del MSPI

Fuente: MinTIC

6.1 FASE DIAGNÓSTICO

En esta fase se utilizó la herramienta de diagnóstico para conocer el estado actual de la seguridad y privacidad de la información de la Universidad, obteniendo los siguientes resultados:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	72	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	80	100	GESTIONADO
A.9	CONTROL DE ACCESO	67	100	GESTIONADO
A.10	CRIPTOGRAFÍA	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	79	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	75	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	80	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	80	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	GESTIONADO
A.18	CUMPLIMIENTO	80	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		78	100	GESTIONADO

Figura 2. Evaluación de efectividad de los controles de la norma ISO 27001:2013 según la herramienta de diagnóstico

Fuente: Elaboración propia

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	24%	40%
	Implementación	4%	20%
	Evaluación de desempeño	5%	20%
	Mejora continua	16%	20%
TOTAL		49%	100%

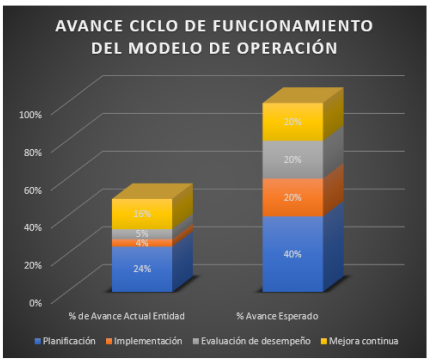

Figura 3. Avance de la implementación del modelo PHVA según la herramienta diagnóstico

Fuente: Elaboración propia

De acuerdo con la Figura 2 y Figura 3, la Universidad de la Amazonia, en su adopción de la política de seguridad de la información, el buen uso de prácticas de protección de datos y capacitación sobre uso de OneDrive para copias de seguridad de información institucional obtiene un 78% de efectividad en la aplicación de estos y un 49% en la retroalimentación de la ejecución del modelo PHVA. Sin embargo, en el levantamiento de requerimientos e información se identificó la inexistencia de algunos documentos necesarios para completar con el modelo MSPI (ver Figura 4).

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

UNIVERSIDAD DE LA AMAZONIA

DATOS BASICOS	
Tipo Entidad	De orden nacional
Misión	descripción
Análisis de Contexto	
Mapa de Procesos	
Organigrama	

PREGUNTAS	
Que le preocupa a la Entidad en temas de seguridad de la	La protección de la información de los beneficiarios desde el punto de vista de la confidencialidad y la integridad.
En que nivel de madurez considera que está?	
En que componente del ciclo PHVA considera que va?	

NO.	DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN Lista de información BASICA a solicitar	NOMBRE DEL DOCUMENTO ENTREGADO	OBSERVACIONES
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)		ENTIDAD DE ORDEN NACIONAL
2	Misión	https://www.uniamazonia.edu.co/inicio/index.php/la-universidad/presentacion/mision-vision.html	
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.		
4	Mapa de Procesos	https://www.uniamazonia.edu.co/documentos/docs/Sistema%20Integrado%20de%20Gestion%20de%20Calidad/5.%20Mapa%20de%20Procesos/Mapa%20de%20Procesos.png	
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	https://www.uniamazonia.edu.co/inicio/index.php/es/la-universidad/organigrama.html	
6	Políticas de seguridad de la información formalizada y firmada	https://www.uniamazonia.edu.co/documentos/docs/Consejo%20Superior/Acuerdos/2017/Acuerdo%20017%20-%20Politicas%20del%20DTI.pdf	
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	https://www.uniamazonia.edu.co/documentos/docs/Consejo%20Superior/Acuerdos/2017/Acuerdo%20017%20-%20Politicas%20del%20DTI.pdf	
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección		
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	Instrumento de evaluación 2026	
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección		No aplica
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)		
12	Procedimientos de control documental del MSPI		
13	Metodología de Gestión de riesgos	https://www.uniamazonia.edu.co/documentos/docs/Sistema%20Integrado%20de%20Gestion%20de%20Calidad/8.%20Administracion%20del%20riesgo/GU-E-AC-11.pdf	
14	Riesgos identificados y valorados de acuerdo a la metodología	https://www.uniamazonia.edu.co/documentos/docs/Sistema%20Integrado%20de%20Gestion%20de%20Calidad/8.%20Administracion%20del%20riesgo/Politica%20de%20Administracion%20de%20Riesgos.pdf	
15	Planes de tratamiento de los riesgos	http://www.uniamazonia.edu.co/documentos/docs/Consejo%20Superior/Acuerdos/2017/Acuerdo%2017%20Politicas%20del%20DTI.pdf	
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información		Las responsabilidades se mencionan en los contratos.
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad		Tarea realizada por DSA.
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.		
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información		Tarea realizada por Secretaria General y DSA.
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección		Tablas de retención documental Aprobadas, en proceso la publicación del inventario de activos de la información.
21	Inventario de áreas de procesamiento de información y telecomunicaciones		
22	Diagrama de red de alto nivel o arquitectura de TI		
23	Inclusión de la seguridad de la información en la gestión de proyectos		
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad		Tarea realizada por Almacén.
25	Formato de acuerdo de transferencia de información		Acuerdo descrito en los contratos.
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden		Tarea realizada por Almacén y Compras.
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.		
28	Plan de continuidad de la Entidad aprobado		
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información		Tarea realizada por Secretaria General.
30	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad		Tarea realizada por Control Interno.
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.	https://www.uniamazonia.edu.co/documentos/docs/Consejo%20Superior/Acuerdos/2017/Acuerdo%20017%20-%20Politicas%20del%20DTI.pdf	Validar cual seria ese enlace.
32	Indicadores y métricas de seguridad de la información definidos.		
33	Declaración de aplicabilidad		
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	https://www.uniamazonia.edu.co/documentos/docs/Sistema%20Integrado%20de%20Gestion%20de%20Calidad/8.%20Administracion%20del%20riesgo/Politica%20de%20Administracion%20de%20Riesgos.pdf	
	Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN		
35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.		
36	Avance en la ejecución del plan de tratamiento de riesgos		
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.		
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO		
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.		
39	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.		
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.		
	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA		
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.		
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.		

Figura 4. Levantamiento de requerimientos e información

Fuente: Elaboración propia

6.2 FASE PLANIFICACIÓN

Teniendo en cuenta los resultados de la fase diagnóstico, se describen las siguientes actividades (ver Tabla 1) para evaluar anualmente los procedimientos, políticas, controles, documentación, entre otros.

PLANIFICACIÓN			
Gestión	**Actividad(es)**	**Responsable**	**Fecha de ejecución**
Política de seguridad de la información	• Divulgación de la política de seguridad de la información.	OATI	Enero 2026 – Diciembre 2026
Políticas de seguridad de la información	• Revisión de las políticas establecidas en la política general de seguridad de la información. • Actualización de los controles de las políticas (en caso de ser necesario). • Incorporación de controles a las políticas según otros estándares de seguridad y ciberseguridad (en caso de ser necesario). • Aprobación de la política de seguridad de la información (en caso de actualización).	OATI	Enero 2026 – Diciembre 2026

	• Divulgación de la política de seguridad de la información.		
Roles y responsabilidades	• Verificación de roles de acceso a equipos de cómputo y Sistema de Información Misional Chairá de los usuarios nuevos y antiguos. • Actualización de políticas de grupo en el directorio activo para restricción de uso e instalación de software (en caso de ser necesario).	OATI	Enero 2026 – Diciembre 2026
Activos de información	• Actualización de documentación relacionada con los activos que brindan servicios tecnológicos de acuerdo a las metodologías de identificación, clasificación y valoración de riesgos. • Divulgación de la documentación respectiva a las partes interesadas.	OATI	Enero 2026 – Diciembre 2026
Riesgos	• Revisión de los riesgos asociados al proceso Gestión Tecnológica. • Revisión de clasificación de los riesgos establecidos en el proceso de Gestión Tecnológica. • Actualización de controles existentes asociados a los riesgos (en caso de ser necesario). • Actualización del plan de tratamiento de riesgos de	OATI	Enero 2026 – Diciembre 2026

	seguridad y privacidad de la información.		
Auditorías internas	• Revisar documentación requerida por la oficina Control Interno sobre auditorías de Calidad. • Verificación de firmas de actas de gestión de solicitudes. • Verificación de respuestas a los incidentes registrados en el módulo de Mesa de Servicios.	OATI	Enero 2026 – Diciembre 2026
Copias de seguridad	• Verificación de copias de seguridad de logs de la plataforma Chairá. • Verificación de copias de seguridad de las bases de datos MySQL y MongoDB. • Verificación de copias de seguridad de los sitios completos del IIS.	OATI	Enero 2026 – Diciembre 2026
Capacitaciones	• Ejecutar plan de mantenimiento de servicios tecnológicos. • Capacitar a los funcionarios administrativos en el uso de OneDrive institucional.	OATI	Enero 2026 – Diciembre 2026

Tabla 1. Planificación de actividades periodo enero 2026 – diciembre 2026

Fuente: Elaboración propia

6.3 FASE IMPLEMENTACIÓN

IMPLEMENTACIÓN			
Gestión	**Entregable(s)**	**Responsable**	**Fecha de ejecución**
Política de seguridad de la información	Divulgación de la política de seguridad de la información.	OATI	Enero 2026 – Diciembre 2026
Políticas de seguridad de la información	Divulgación de las políticas asociados a la política general de seguridad de la información.	OATI	Enero 2026 – Diciembre 2026
Roles y responsabilidades	Informe de revisión y actualización de roles y responsabilidades de los usuarios nuevos y antiguos.	OATI	Enero 2026 – Diciembre 2026
Activos de información	Documento de activos de información.	OATI	Enero 2026 – Diciembre 2026
Riesgos	• Informe de revisión y actualización de riesgos del proceso Gestión Tecnológica. • Informe de revisión y actualización del	OATI	Enero 2026 – Diciembre 2026

	plan de tratamiento de riesgos de seguridad de la información.		
Auditorías internas	Informe de resultados de auditoría de calidad.	Control Interno	Enero 2026 – Diciembre 2026
Copias de seguridad	Copias de seguridad subidas a la nube.	OATI	Enero 2026 – Diciembre 2026
Capacitaciones	Informe de personal capacitado en la Universidad.	OATI	Enero 2026 – Diciembre 2026

Tabla 2. Implementación y productos entregables según las actividades planeadas periodo enero 2026 – diciembre 2026.
Fuente: Elaboración propia

6.4 FASE EVALUACIÓN

EVALUACIÓN			
Gestión	**Resultado(s)**	**Responsable**	**Fecha de ejecución**
Política de seguridad de la información	Validación de la divulgación de la política de seguridad de la información.	OATI	Enero 2026 – Diciembre 2026
Políticas de seguridad de la información	Validación de la divulgación de las políticas asociadas a la	OATI	Enero 2026 – Diciembre 2026

	política general de seguridad de la información.		
Roles y responsabilidades	Aprobación del informe de revisión y actualización de roles y responsabilidades de los usuarios nuevos y antiguos.	OATI	Enero 2026 – Diciembre 2026
Activos de información	Documento aprobado de activos de información.	OATI	Enero 2026 – Diciembre 2026
Riesgos	• Aprobación informe de revisión y actualización de riesgos del proceso Gestión Tecnológica. • Aprobación de informe de revisión y actualización del plan de tratamiento de riesgos de seguridad de la información.	OATI	Enero 2026 – Diciembre 2026
Auditorías internas	Plan de mejoramiento según el formato establecido por el SIGC.	OATI	Enero 2026 – Diciembre 2026

Copias de seguridad	Acta de verificación de las copias de seguridad subidas a la nube.	OATI	Enero 2026 – Diciembre 2026
Capacitaciones	Aprobación del informe de personal capacitado en la Universidad.	OATI	Enero 2026 – Diciembre 2026

Tabla 3. Evaluación de los productos entregables periodo enero 2026 – diciembre 2026

Fuente: Elaboración propia

6.5 FASE MEJORA CONTINUA

EVALUACIÓN			
Gestión	**Resultado(s)**	**Responsable**	**Fecha de ejecución**
Política de seguridad de la información	Revisión de limitaciones y observaciones según el informe presentado en la fase anterior.	OATI	Enero 2026 – Diciembre 2026
Políticas de seguridad de la información	Revisión de limitaciones y observaciones según el informe presentado en la fase anterior.	OATI	Enero 2026 – Diciembre 2026
Roles y responsabilidades	Revisión de limitaciones y observaciones según el informe presentado en la fase anterior.	OATI	Enero 2026 – Diciembre 2026
Activos de información	Revisión de limitaciones y observaciones de la	OATI	Enero 2026 – Diciembre 2026

	elaboración del documento de activos de información.		
Riesgos	Revisión de limitaciones y observaciones de la revisión y actualización de riesgos del proceso de Gestión Tecnológica y Plan de tratamiento de riesgos de seguridad de la información.	OATI	Enero 2026 – Diciembre 2026
Auditorías internas	Revisión de los hallazgos de la auditoría realizada.	OATI	Enero 2026 – Diciembre 2026
Copias de seguridad	Revisión de limitaciones y observaciones de la realización de las copias de seguridad.	OATI	Enero 2026 – Diciembre 2026
Capacitaciones	Revisión de limitaciones y observaciones del personal no capacitado en la Universidad.	OATI	Enero 2026 – Diciembre 2026

Tabla 4. Mejora continua de los productos entregados periodo enero 2026 – diciembre 2026
Fuente: Elaboración propia

6.6 LIMITACIONES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

- Inexistencia de procedimientos, políticas y controles documentados.
- Falta de talento humano capacitado para realizar la revisión de la documentación.
- Ocurrencia de imprevistos ajenos en las fases del plan.

7 ANEXO

7.1 ANEXO 1. PLAN DE MEJORAMIENTO AUDITORÍA DE CALIDAD 2026-1

	FORMATO PLAN DE MEJORAMIENTO POR PROCESOS					
	CÓDIGO: FO-E-GC-02-05		VERSIÓN: 6		FECHA: 13-03-2026	PÁGINA: 1 de 1

PROCESO:	Gestión Tecnologica
GESTOR DEL PROCESO:	Jairo Andres Durango Hernandez
PERIODO AUDITADO:	2025
FECHA DE SUSCRIPCIÓN	14/03/2026

CRITERIO	DESCRIPCIÓN DE LA NO CONFORMIDAD	CAUSA DE LA NO CONFORMIDAD	ACCIÓN CORRECTIVA	META	FECHA DE INICIO	FECHA DE TERMINACION	RESPONSABLE ACCIÓN CORRECTIVA
PD-S-AC-11 Numeral 11.1 ISO 9001:2015 Requisitos 7.5.2, 10.3 ISO 21001:2018 Requisitos 7.5.2,10.2	Durante el desarrollo de la auditoría no se evidenció el formato FO-S-AC-11-01 para la modificación de los formatos Historia de Usuario FO-A-GT-02-01 y Formato de Pruebas de Software FO-A-GT-02-02	Se evidencian oportunidades de fortalecimiento en los mecanismos de control y verificación asociados a la aplicación de los lineamientos para la elaboración y modificación de documentos, teniendo en cuenta que no se realizó la verificación específica del diligenciamiento del formato FO-S-AC-11-01, al asumirse que las modificaciones de los formatos se encontraban inmersas dentro del cambio del procedimiento asociado al Desarrollo Tecnologico y cubiertas con el diligenciamiento del formato asociado a dicho cambio.	Diligenciar y enviar el formato FO-S-AC-11-01 correspondiente a las modificaciones realizadas, remitido a la dependencia de Aseguramiento de la Calidad.	Asegurar la aplicación del formato FO-S-AC-11-01 en la totalidad de las modificaciones documentales realizadas, conforme a los lineamientos definidos.	14/03/2026	14/07/2026	Profesional Universitario
Ley 594 de 2000 Acuerdo 01/2024 Consejo Directivo del Archivo General de la Nación. Norma ISO 9001:2015 Requisitos 7.5.3 y 7.5.3.2 ISO 21001:2018 Requisitos 7.5.3, 7.5.3.2 GU-A-GD-01 guía de implementación de las tablas de retención documental	Durante la auditoría se evidenció que las comunicaciones oficiales de la vigencia 2025 no se encuentran organizadas de forma cronológica, no están foliadas y no cuentan con hoja de control. Además, presentan archivo pendiente para transferir desde la vigencia 2012.	Se evidencian oportunidades de fortalecimiento en la aplicación y control de los lineamientos establecidos para la gestión documental, asociadas a la ausencia de mecanismos de organización, seguimiento y verificación que garanticen la adecuada clasificación, orden y transferencia de las comunicaciones oficiales.	1. Solicitar formalmente a la dependencia de archivo los lineamientos para el rótulo y organización de las Comunicaciones Oficiales Internas, dejando evidencia de cada solicitud y respuesta recibida. 2. Implementar el uso de dichos lineamientos en la organización de las comunicaciones oficiales del área. 3. Realizar la revisión, organización cronológica y foliación del archivo de Comunicaciones Oficiales Internas de las futura vigencias. 4. Gestionar la transferencia documental correspondiente, incluyendo el archivo pendiente desde la vigencia 2012, conforme a las tablas de retención documental.	Asegurar la correcta organización, clasificación, orden cronológico y control de las Comunicaciones Oficiales Internas, así como la transferencia documental del archivo de la Oficina Asesora de Tecnologías de la Información (OATI), conforme a los lineamientos de gestión documental y tablas de retención documental vigentes.	14/03/2026	14/07/2026	Profesional Universitario
Acuerdo 086 del 2024 C.S.U. articulo 59 numeral 5 Circular 017 de 15 de agosto de 2023, circular 003 del 27 de febrero de 2024, 002 del 02/02/2026 de la Dirección GTH. ISO 9001:2015 e ISO 21001:2018 Requisito 4.1	Durante la verificación en campo realizada a las diferentes áreas de la dependencia, se observó que varios funcionarios no portaban el carné institucional en el desarrollo de sus actividades laborales. Esta situación se presentó en distintos momentos de la auditoría y resultó reiterativa, a pesar de que en el informe final de la auditoría del año anterior ya se había dejado como una oportunidad de mejora por el incumplimiento de esta obligación.	Se evidencian oportunidades de fortalecimiento en los mecanismos de seguimiento y control asociados al cumplimiento de los lineamientos institucionales sobre el uso del carné institucional, teniendo en cuenta que no se han consolidado verificaciones sistemáticas que aseguren su aplicación continua durante la jornada laboral, lo que ha incidido en la reiteración de la situación previamente identificada.	1. Socializar nuevamente a los funcionarios los lineamientos institucionales relacionados con el uso obligatorio del carné institucional durante la jornada laboral. 2. Implementar un mecanismo de verificación periódica (listas de chequeo o controles aleatorios) por parte de los líderes de área para supervisar el cumplimiento de esta obligación.	Lograr el uso permanente del carné institucional por parte de los funcionarios durante la jornada laboral.	14/03/2026	14/07/2026	Profesional Universitario

Ley 1581 de 2012 Art 4 literales G y H Art 17 literales A - D Decreto 767 de 2022 Art. 2.2.9.1.1.3 Acuerdo No. 17 del 2017 (Política DTI – política de seguridad física) página 5 ISO 9001:20015 8.1 literal d ISO 21001:2018 Requisito 8.1	Durante la verificación realizada en el transcurso de la auditoria, se evidenció que la dependencia no cuenta con sistemas de seguridad para impedir el acceso a lugares de acceso restringido, tales como áreas de servidores principales y telecomunicaciones. Adicionalmente, al revisar el registro de ingresos se identificó que en el libro radicador figura el ingreso de un externo el 04/11/2025 para adelantar actividades de revisión y diagnóstico del servicio de internet, sin que exista evidencia de acompañamiento por parte de un funcionario.	Se identifican oportunidades de fortalecimiento en la implementación de controles de acceso físico a áreas restringidas, relacionadas con la ausencia de medidas de seguridad y de lineamientos operativos que aseguren la restricción, registro, verificación y acompañamiento del ingreso de personal interno y externo a dichas áreas.	1. Implementar medidas de seguridad física para restringir el acceso a áreas de acceso controlado (servidores y telecomunicaciones), mediante la definición e instalación de mecanismos que limiten el ingreso a personal autorizado. 2. Establecer y formalizar el control de ingreso de personal interno y externo mediante la implementación de un libro radicador, el cual deberá contener en su registro: nombre del visitante, entidad, motivo de ingreso, fecha, hora, firma y funcionario responsable del acompañamiento. 3. Disponer de libros de registro en cada uno de los puntos donde se encuentren ubicados los servidores, con el fin de garantizar la trazabilidad de los accesos. 4. Definir e implementar un instructivo para el control de acceso a áreas restringidas, incluyendo la obligatoriedad del acompañamiento por parte de un funcionario de la OATI durante la permanencia de personal externo. 5. Articular el instructivo definido con el procedimiento de mantenimiento de equipos de cómputo, asegurando su aplicación en todas las intervenciones técnicas realizadas.	Asegurar la restricción, control y trazabilidad del acceso a las áreas de servidores y telecomunicaciones, mediante la implementación de medidas de seguridad, el registro de ingresos y la aplicación de lineamientos que garanticen el acompañamiento del personal autorizado.	14/03/2026	14/07/2026	Profesional Universitario
ISO 9001:20015 8.1 literal d ISO 21001:2018 Requisito 8.1 Acuerdo No. 17 del 2017 (Política DTI) PAGINA 6	En el transcurso de la auditoria, se evidenció que la dependencia no cuenta con los planos actualizados de las instalaciones eléctricas y de comunicaciones correspondientes a diferentes construcciones de la Institución. Se verificó que los planos disponibles no incluyen las edificaciones recientes, entre ellas el Edificio Tucán de la sede principal y las nuevas construcciones en las sedes Santo Domingo y Macagual. Cabe señalar que esta situación ya había sido señalada en la auditoria de la vigencia anterior como una oportunidad de mejora, motivo por el cual pasa a constituirse en NO conformidad.	Se evidencian oportunidades de fortalecimiento en la gestión y articulación institucional para la consolidación y actualización de la información técnica relacionada con planos eléctricos y de comunicaciones, asociadas a la disponibilidad parcial de dicha información por parte de las dependencias responsables, lo que ha limitado su actualización integral.	Solicitar formalmente a la Oficina Asesora de Planeación la información actualizada de los planos eléctricos y de comunicaciones disponibles para las diferentes sedes de la Institución, dejando evidencia de las solicitudes realizadas.	Contar con los planos actualizados de las instalaciones eléctricas y de comunicaciones de todas las construcciones de la Institución, incluyendo el Edificio Tucán de la sede principal y las nuevas construcciones en las sedes Santo Domingo y Macagual, dejando evidencia de su disponibilidad y verificación por la dependencia responsable.	14/03/2026	14/07/2026	Profesional Universitario
Manual de Gobierno Digital Anexo 2 – pág. 77 Resolución 1126 de 2021 "Por la cual se modifica la Resolución 2710 de 2017, por la cual se establecen lineamientos para la adopción del protocolo IPv6" ISO 9001:20015 Requisito 7.5 ISO 21001:2018 Requisito 7.5	Se evidencia incumplimiento al Artículo 1 de la Resolución 1126 de 2021 MINTIC, la cual establece que las entidades estatales del orden nacional deberán culminar el proceso de transición al protocolo IPv6, en convivencia con el protocolo IPv4 a más tardar el 30 de junio de 2022. En auditoría realizada a la vigencia 2022 se establece la NO conformidad, siendo esta reiterativa.	No se completó la transición al protocolo IPv6 en convivencia con IPv4 debido a la disponibilidad parcial de los recursos y la información técnica necesarios, así como a la ausencia de mecanismos de seguimiento que aseguren la implementación oportuna del proceso.	Ejecución de la Fase III. Pruebas de Funcionalidad, en el proceso de transicción de IPv4 a IPv6.	Verificar y validar la correcta implementación de IPv6 en la infraestructura de red, asegurando la funcionalidad, conectividad, compatibilidad y rendimiento de los servicios, mediante la ejecución completa de las **pruebas de funcionalidad** correspondientes en la fase final del proceso de transición.	14/03/2026	14/07/2026	Profesional Universitario
Ley 1581 de 2012 Art 4 literal G, Art 17 literal D ISO 9001:20015 8.1 literal d ISO 21001:2018 Requisito 8.1 Acuerdo No. 17 del 2017 (Política DTI) página 13	No existe registro del inventario de medios magnéticos, a pesar de que la política institucional establece la obligatoriedad de identificar, registrar y controlar estos elementos como parte de las medidas destinadas a prevenir la pérdida, deterioro o alteración de la información almacenada.	Se evidencian oportunidades de fortalecimiento en la gestión y control de los medios magnéticos, ya que, aunque estos se encuentran inmersos dentro del inventario general de bienes e inmuebles, no existe un registro individualizado que permita identificarlos, controlarlos y darles seguimiento de manera específica, tal como lo establece la política institucional para prevenir la pérdida, deterioro o alteración de la información.	Implementar un inventario exclusivo de medios magnéticos, que permita su identificación, control y seguimiento de manera individual, conforme a la política institucional.	Contar con un inventario individualizado de medios magnéticos actualizado, que permita su identificación, control y seguimiento, asegurando la protección de la información según la política institucional.	14/03/2026	14/07/2026	Profesional Universitario

ISO 9001:20015 ISO 21001:2018 4.4.1 literal F y 6.1 OD-S-AC-15-01 resolución 0886 del 2007	Durante la verificación realizada en el proceso de auditoria se evidenció que no existe evidencia de la socialización de los instructivos de uso del software, pese a que dicha actividad hace parte de las acciones de tratamiento establecidas para el riesgo denominado "Fallas de Software".	Se evidencian oportunidades de fortalecimiento en la gestión y articulación institucional, ya que no se cuenta con evidencia de la socialización de los instructivos de uso del software, debido a la ausencia de un mecanismo formal que asegure la comunicación y capacitación de los usuarios sobre las acciones de tratamiento del riesgo "Fallas de Software"	Realizar la socialización formal de los instructivos de uso del software a todos los usuarios correspondientes, dejando evidencia documentada de la actividad (asistencias, actas o registros digitales), y establecer un mecanismo de seguimiento para asegurar que esta socialización se realice de manera periódica y oportuna.	Garantizar que todos los usuarios del software reciban la socialización de los instructivos de uso, dejando evidencia documentada de la actividad y asegurando la implementación oportuna de las acciones de tratamiento del riesgo "Fallas de Software"	14/03/2026	14/07/2026	Profesional Universitario
ISO 9001:20015 e ISO 21001:2018 Requisitos 4.4.1 literal F y 6.1 Matriz riesgos de corrupción Ley 1474 de 2011 articulo 73.	Durante la verificación realizada en el proceso auditor se evidenció que no existe la Política de Seguridad de la Información y Operaciones, ni evidencias de su implementación. Esta situación afecta la gestión de varios riesgos de corrupción, dado que dicho documento constituye un control preventivo fundamental para mitigar, entre otros, los siguientes riesgos: • Ejecución de acciones CRUD de usuarios autorizados. • Pérdida de información en los sistemas de información y bases de datos. • Acceso no autorizado a la infraestructura tecnológica. • Divulgación de información reservada relacionada con seguridad de la información.	Se evidencian oportunidades de fortalecimiento en la gestión de seguridad de la información, debido a la ausencia de la Política de Seguridad de la Información y Operaciones, lo que impide contar con un respaldo formal para la mitigación de riesgos asociados a corrupción, acceso no autorizado, pérdida de información y divulgación de información reservada.	Elaborar el diagnostico de la Política de Seguridad de la Información y Operaciones, asegurando su socialización a las áreas pertinentes y su vinculación con los riesgos institucionales, incluyendo mecanismos de seguimiento y actualización periódica.	Contar con un diagnostico de la Política de Seguridad de la Información	14/03/2026	14/07/2026	Profesional Universitario
ISO 9001:20015 e ISO 21001:2018 4.4.1 literal F y 6.1 Matriz riesgos de corrupción Ley 1474 de 2011 articulo 73.	Durante la auditoría no se evidenció trazabilidad ni registros completos sobre la solicitud de copia de seguridad realizada por el Departamento de Gestión del Talento Humano el 16 de octubre de 2025, ya que no se encontró evidencia de su ejecución, verificación, documentación o cierre. Así mismo, se verificó que en junio de 2025 ocurrió un incidente de seguridad que afectó la página institucional mediante creación de usuarios y alteración visual, sin que existiera registro, reporte, análisis o documentación del tratamiento del incidente.	Se evidencian oportunidades de fortalecimiento en la gestión de copias de seguridad e incidentes de seguridad, debido a la ausencia de trazabilidad y registros completos de las solicitudes y eventos, lo que impide verificar la ejecución, seguimiento y cierre de las actividades conforme al procedimiento institucional.	1. Actualización del procedimiento: Revisar y actualizar el procedimiento de copias de seguridad, incorporando controles claros para solicitud, ejecución, verificación, documentación y cierre de las copias. 2 Registro y trazabilidad: Definir el sistema o mecanismo que permita llevar trazabilidad completa de cada solicitud de copia de seguridad y de los incidentes de seguridad asociados. 2. Capacitación y socialización: Socializar el procedimiento actualizado a los responsables de la ejecución y verificación de copias de seguridad, asegurando que conozcan sus obligaciones y registros requeridos.	Contar con registros completos y trazables de todas las solicitudes de copias de seguridad e incidentes de seguridad, gestionados conforme al procedimiento actualizado, asegurando la ejecución, verificación, documentación y cierre adecuados de cada actividad.	14/03/2026	14/07/2026	Profesional Universitario
ISO 9001:20015 e ISO 21001:2018 4.4.1 literal F y 6.1 Matriz riesgos de corrupción Ley 1474 de 2011 articulo 73.	Durante la auditoría se evidenció que no se cuenta con mecanismos de autenticación biométrica para el ingreso a recursos físicos asociados a la infraestructura tecnológica, a pesar de estar definidos como control preventivo para mitigar el riesgo de acceso no autorizado a la infraestructura tecnológica.	Se evidencian oportunidades de fortalecimiento en la gestión de seguridad física de la infraestructura tecnológica, debido a la ausencia de mecanismos de autenticación biométrica para el control de acceso, lo que limita la efectividad de los controles preventivos establecidos en la matriz de riesgos.	1. Revisar la matriz de riesgos e identificar si se requiere actualizar el control de acceso biométrico como medida preventiva prioritaria. 2. Evaluar, seleccionar e implementar soluciones de autenticación biométrica para el acceso a la infraestructura tecnológica, incluyendo su instalación, puesta en operación y la ejecución de pruebas de funcionamiento para ajustar. 3. Socialización y seguimiento, capacitar al personal autorizado sobre el uso de los mecanismos y establecer un plan de seguimiento para verificar su efectividad.	Contar con mecanismos de autenticación biométrica implementados y operativos para el acceso a la infraestructura tecnológica, respaldados en la matriz de riesgos actualizada, asegurando la prevención de accesos no autorizados.	14/03/2026	14/07/2026	Profesional Universitario
ISO 9001:20015 e ISO 21001:2018 4.4.1 literal F y 6.1 Matriz riesgos de corrupción Ley 1474 de 2011 articulo 73	No existe evidencia que el jefe de la dependencia, en calidad de supervisor de contratos, haya recibido capacitaciones periódicas en el manual de contratación, a pesar de que este control está definido para mitigar los riesgos de corrupción relacionados con: • Omisión de obligaciones contractuales en servicios o productos TI, y • Evaluación de cotizaciones en calidad de supervisor de los contratos.	Se evidencian oportunidades de fortalecimiento en la implementación y control de las capacitaciones asociadas al manual de contratación, debido a debilidades en la periodicidad, seguimiento y registro de las mismas, lo que ha generado la ausencia de evidencia documental que demuestre el cumplimiento del control establecido.	Actualizar la matriz de riesgos de corrupción, así como verificar la eficacia del control definido para la supervisión contractual, incluyendo su aplicación, seguimiento y la existencia de evidencias que respalden su cumplimiento; y, en caso de identificarse controles que no sean del ámbito de competencia de la dependencia, realizar su ajuste o redefinición dentro de la matriz de riesgos.	Contar con la matriz de riesgos de corrupción actualizada y con el control de la supervisión contractual verificado en cuanto a su eficacia, asegurando la existencia de evidencias que respalden su aplicación y seguimiento; y, en caso de identificarse controles que no sean del ámbito de competencia de la dependencia, realizar su ajuste o redefinición dentro de la matriz de riesgos.	14/03/2026	14/07/2026	Profesional Universitario

PD-A-GT-01 ISO 9001:2015 e ISO 21001:2018 Requisito 8.1	Durante el desarrollo de la auditoria se evidenció el incumplimiento del objetivo establecido en el procedimiento de mantenimiento preventivo de plataformas institucionales y bases de datos, debido a que no existe planificación documentada del mantenimiento preventivo de bases de datos para la vigencia 2025.	Se evidencian oportunidades de fortalecimiento en la planificación y control del mantenimiento preventivo de plataformas institucionales, específicamente en la documentación y registro del mantenimiento de bases de datos, lo que generó la ausencia de evidencia formal que demuestre su programación y ejecución durante la vigencia 2025.	Establecer y documentar la planificación del mantenimiento preventivo de plataformas institucionales y bases de datos, asegurando su inclusión dentro de los instrumentos de seguimiento definidos (cronograma, solicitud e informe), así como la consolidación de evidencias que respalden su ejecución durante la vigencia.	Contar con la planificación documentada del mantenimiento preventivo de plataformas institucionales y bases de datos, así como con registros e informes que evidencien su ejecución correcta y seguimiento durante la vigencia.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-01 Numeral 1.1 y 1.2 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció el incumplimiento de la obligación de solicitar el mantenimiento preventivo a todos los coordinadores encargados de administrar las plataformas y bases de datos, debido a que la solicitud realizada por la dependencia no incluyó la totalidad de las plataformas institucionales, particularmente la página web editorial, pese a que estas hacen parte del alcance del procedimiento. Esta situación ya había sido señalada como oportunidad de mejora en la auditoría del año anterior y, al persistir, se constituye en NO conformidad.	Se evidencian oportunidades de fortalecimiento en la asignación de responsabilidades y en el control del proceso de solicitud de mantenimiento preventivo, dado que, si bien se ejecutaron los mantenimientos correspondientes, se presentaron debilidades en la asignación adecuada de los responsables y en la consolidación de la información, lo que ocasionó la omisión de algunos componentes como las bases de datos, así como la inclusión de plataformas institucionales que no son objeto de mantenimiento directo por parte de la Oficina Asesora de Tecnologías de la Información, generando inconsistencias en la trazabilidad y validez del informe.	1. Asignar el caso al responsable del mantenimiento de bases de datos y de cada una de las plataformas institucionales bajo el alcance de la Oficina Asesora de Tecnologías de la Información. 2. Crear un informe consolidado de las plataformas institucionales objeto de mantenimiento por parte de la Oficina (Página web institucional – Periódico Institucional, Sistema de Información Misional Chairá, Aula Extendida y Campus Virtual), documentando en este la ejecución del mantenimiento preventivo y evidenciando la totalidad de las plataformas y bases de datos bajo responsabilidad.	Contar con la asignación formal de responsables del mantenimiento de bases de datos y plataformas institucionales, así como con un informe consolidado que evidencie la ejecución del mantenimiento preventivo, incluyendo la totalidad de las plataformas y bases de datos bajo responsabilidad de la Oficina Asesora de Tecnologías de la Información.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-01 Numeral 1.3 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la verificación realizada en el proceso auditor se evidenció que no se efectuó la asignación de responsables conforme a lo establecido en el procedimiento para el mantenimiento preventivo de plataformas institucionales y bases de datos. En lugar de designar a los responsables específicos para cada tipo de mantenimiento según corresponda a la Plataforma Misional Chairá, Aula Extendida o bases de datos Oracle, solo se asignó como responsable a la Ingeniera Paola Andrea Rodríguez Betancourth, coordinadora de bases de datos, sin diferenciar las actividades ni designar a los demás coordinadores que el procedimiento contempla.	Se evidencian oportunidades de fortalecimiento en la asignación de responsabilidades para el mantenimiento preventivo de plataformas institucionales y bases de datos, debido a la ausencia de un mecanismo formal que garantice la diferenciación de roles conforme a los tipos de mantenimiento definidos en el procedimiento, así como debilidades en el control de su aplicación, lo que generó una asignación generalizada sin distinción de actividades específicas.	Realizar la correcta asignación de los responsables del mantenimiento preventivo de plataformas institucionales y bases de datos conforme a lo establecido en el procedimiento, asegurando la diferenciación de roles según el tipo de mantenimiento.	Contar con la correcta asignación de responsables para el mantenimiento preventivo de plataformas institucionales y bases de datos conforme a lo establecido en el procedimiento, diferenciados según el tipo de mantenimiento y con evidencia documentada de su designación.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-01 Numeral 1.4 y 1.5 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que los mantenimientos preventivos no fueron documentados conforme al procedimiento, ya que el informe presentado no cuenta con la firma del responsable, lo cual impide validar la ejecución y cierre formal de la actividad. Adicionalmente, dicho informe registra como responsable a Yhefferson Huaca, pese a que en Mesa de Servicios la asignación formal del mantenimiento fue realizada a la Ingeniera Paola Andrea Rodríguez Betancourth, coordinadora de bases de datos. Esta inconsistencia genera que el informe carezca de validez como evidencia del mantenimiento realizado.	Se evidencian oportunidades de fortalecimiento en la asignación de responsabilidades para el mantenimiento preventivo de plataformas institucionales y bases de datos, debido a la ausencia de un mecanismo formal que garantice la diferenciación de roles conforme a los tipos de mantenimiento definidos en el procedimiento, así como debilidades en el control de su aplicación, lo que generó una asignación generalizada sin distinción de actividades específicas.	Realizar la correcta documentación del mantenimiento preventivo de plataformas institucionales y bases de datos conforme a lo establecido en el procedimiento, asegurando la diferenciación de roles según el tipo de mantenimiento.	Contar con la correcta documentación del mantenimiento preventivo de plataformas institucionales y bases de datos conforme a lo establecido en el procedimiento, diferenciados según el tipo de mantenimiento y con evidencia documentada de su designación.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-02 numeral 2.1 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que, para la vigencia 2025, no existe registro de solicitud de desarrollo tecnológico para el servicio de facturación enviada a Mesa de Servicios, pese a que el procedimiento establece este canal como la vía oficial para iniciar cualquier requerimiento de desarrollo.	Se evidencian oportunidades de fortalecimiento en el uso del canal oficial para la recepción de solicitudes de desarrollo tecnológico, debido a que se han recepcionado requerimientos a través de correos internos de la oficina, en lugar de utilizar la Mesa de Servicios conforme al procedimiento establecido, lo que ocasionó la falta de registro formal y afectó la trazabilidad de las solicitudes.	Garantizar que todas las solicitudes de desarrollo tecnológico sean gestionadas exclusivamente a través de la Mesa de Servicios como canal oficial, conforme al procedimiento establecido, mediante la socialización del mismo y la implementación de controles que impidan la recepción y atención de requerimientos por canales no autorizados, como el correo interno de la oficina.	Contar con el registro documentado de las solicitudes de desarrollo tecnológico gestionadas a través de la Mesa de Servicios, conforme al procedimiento establecido, y con mecanismos de control que garanticen la trazabilidad de los requerimientos.	14/03/2026	14/07/2026	Profesional Universitario

PD-A-GT-02 numeral 2.2 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no existe evidencia de la socialización de la solicitud de desarrollo tecnológico entre el Asesor de la OATI y el Coordinador del área de Desarrollo e Investigaciones, pese a que esta actividad es obligatoria para establecer la prioridad y viabilidad del requerimiento	Se evidencian oportunidades de fortalecimiento en la documentación de las actividades asociadas a la gestión de solicitudes de desarrollo tecnológico, debido a que la socialización entre el Asesor de la OATI y el Coordinador del área de Desarrollo e Investigaciones se realiza de manera verbal, sin generar registros formales, lo que ocasionó la ausencia de evidencia del proceso y afecta la trazabilidad en la definición de la prioridad y viabilidad de los requerimientos.	Establecer y asegurar la documentación del proceso de socialización de las solicitudes de desarrollo tecnológico mediante el registro formal en formato de acta, dejando soporte y trazabilidad de la solicitud.	Contar con actas debidamente diligenciadas que documenten la socialización de las solicitudes de desarrollo tecnológico, garantizando el soporte y la trazabilidad de cada solicitud.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-02 numeral 2.5 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	No se encontró a fecha de la auditoría registro del acta FO-S-GJ-16-01 que debe elaborarse para documentar la asignación del personal responsable del desarrollo tecnológico y las tareas iniciales del proceso, conforme a lo dispuesto en el procedimiento. La ausencia de este registro impide verificar la designación formal de roles y funciones para el inicio del desarrollo.	Se evidencian oportunidades de fortalecimiento en la documentación de la asignación de responsabilidades para el inicio del desarrollo tecnológico, debido a debilidades en el cumplimiento del procedimiento establecido, específicamente en la elaboración del acta FO-S-GJ-16-01, lo que ocasiona la ausencia de registro formal para la designación de roles y funciones y afecta la trazabilidad del proceso.	Establecer y asegurar la elaboración del acta FO-S-GJ-16-01 para documentar la asignación del personal responsable del desarrollo tecnológico y las tareas iniciales del proceso, conforme al procedimiento establecido, garantizando su diligenciamiento, aprobación y archivo como evidencia formal.	Contar con el acta FO-S-GJ-16-01 debidamente diligenciada, aprobada y archivada como soporte de la asignación de responsables y de las tareas iniciales del desarrollo tecnológico, conforme al procedimiento establecido, garantizando la trazabilidad del proceso.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-02 numeral 2.7. 2.10 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no existen registros de los informes periódicos que el ingeniero o grupo desarrollador debe presentar al Coordinador del área de Desarrollo e Investigaciones sobre el avance del proceso. Así mismo, no se encontró evidencia de la socialización de dichos avances con el responsable de la solicitud, pese a estar contemplado como parte del procedimiento para garantizar el seguimiento y validación del desarrollo tecnológico.	Actualizar el procedimiento de desarrollo tecnológico, ajustando el paso de seguimiento del avance para definir lineamientos claros sobre el mecanismo de control y documentación del proceso, incorporando el uso del informe final consolidado y las actas como soporte de socialización intermedia, garantizando la trazabilidad y validación del desarrollo.	Actualizar el procedimiento de desarrollo tecnológico para ajustar el paso de seguimiento del avance, definiendo lineamientos claros sobre la generación, periodicidad y socialización de los informes, de acuerdo con la práctica adoptada o el modelo que se establezca.	Contar con el procedimiento de desarrollo tecnológico actualizado, así como con registros documentados que evidencien la aplicación del mecanismo de seguimiento definido, mediante el uso de actas de socialización y un informe final consolidado, garantizando la trazabilidad y validación del proceso.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-02 numeral 2.15 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	No existe evidencia de la capacitación realizada por el ingeniero o grupo desarrollador a las partes interesadas sobre el manejo y funcionamiento del desarrollo implementado, pese a que esta actividad es una etapa obligatoria dentro del procedimiento de desarrollo tecnológico.	Se evidencian oportunidades de fortalecimiento en la documentación de las actividades de capacitación asociadas al desarrollo tecnológico, debido a la ausencia de registros formales de asistencia, pese a que las capacitaciones se realizan, lo que impide evidenciar su ejecución y afecta la trazabilidad del proceso conforme al procedimiento establecido.	Aplicar el formato FO-S-GJ-16-02 para el registro de asistencia a las capacitaciones realizadas por el ingeniero o grupo desarrollador, asegurando su diligenciamiento, generación y conservación como evidencia conforme al procedimiento establecido.	Garantizar que todas las capacitaciones realizadas por el ingeniero o grupo desarrollador queden registradas mediante el formato FO-S-GJ-16-02, debidamente diligenciado, generado y conservado como evidencia, asegurando su uso obligatorio en todas las sesiones y cumpliendo con el procedimiento establecido.	14/03/2026	14/07/2026	Profesional Universitario

PD-A-GT-05 numeral 5.1 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5 Acuerdo No. 18 de 2017 Artículo 7.	Durante la auditoría se evidenció que la planificación del mantenimiento preventivo para la vigencia 2025 no incluyó todas las dependencias de la Universidad, ni contempló las sedes ubicadas en otros departamentos. Así mismo, no se evidenció programación semestral para las salas de sistemas y no existen registros que justifiquen la no realización del mantenimiento en las siguientes dependencias: • Supervisión Campus Centro • Maestría en Administración • Maestría en Tributación • Observatorio Sociopolítico (Sede Centro) • Laboratorios de Ictiología • Centro de Investigación Macagual • Campus Yarí • Oficina Asesora de Planeación • Especializaciones Facultad de Derecho • Programa de Medicina Veterinaria y Zootecnia • Licenciatura en Educación Artística y Cultural • Licenciatura en Literatura y Lengua Castellana • Licenciatura en Educación Física, Deporte y Recreación • Centro de Impresiones • Laboratorio Interactivo de Idiomas • Programa de Química • Programa de Biología • Maestría en Ciencias Biológicas • Laboratorio de Inglés • Ayudas Audiovisuales • Salas de Conferencias Campus Porvenir	Se evidencian oportunidades de fortalecimiento en la prestación del servicio de mantenimiento de equipos de cómputo, dado que, por temas de tiempo y la elevada demanda de solicitudes de incidencias en el área de Hardware, el equipo de soporte técnico no culminó lo establecido en el cronograma, afectando la planeación conforme el procedimiento establecido.	Ajustar el cronograma de mantenimiento de equipos de cómputo, priorizando los espacios físicos a los cuales no se les brindó el servicio, garantizando la cobertura completa y oportuna de todas las dependencias conforme al procedimiento establecido.	Contar con un cronograma de mantenimiento actualizado y ejecutado que asegure la prestación oportuna del servicio a todas las dependencias y sedes de la Universidad, garantizando la operatividad de los equipos conforme al procedimiento.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-05 numeral 5.2 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no se realizó el registro del caso correspondiente al segundo semestre de 2025 para el mantenimiento de elementos tecnológicos en el módulo de Mesa de Servicios de la plataforma Chairá, tal como lo establece el procedimiento.	Se evidencian oportunidades de fortalecimiento en el registro de los casos de mantenimiento de elementos tecnológicos, dado que durante la auditoría se identificó que solo se realizó un registro anual del proceso, en lugar de los registros semestrales establecidos en el procedimiento para el módulo de Mesa de Servicios de la plataforma Chairá.	Ajustar el registro de los casos de mantenimiento de elementos tecnológicos en el módulo de Mesa de Servicios de la plataforma Chairá, asegurando que se realicen de manera semestral conforme al procedimiento establecido.	Contar con registros semestrales de los casos de mantenimiento de elementos tecnológicos en el módulo de Mesa de Servicios del Sistema de Información Misional Chairá, garantizando la trazabilidad y cumplimiento del procedimiento.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-05 numeral 5.4 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que el mantenimiento preventivo de los equipos de cómputo no se realiza conforme al instructivo IN-A-GT-05-01, ya que no se ejecutan actividades básicas contempladas en el mantenimiento, tales como la limpieza de teclados, mouse y pantallas. Adicionalmente, se constató que los instructivos IN-A-GT-05-02, IN-A-GT-05-03 e IN-A-GT-05-04, referenciados en el procedimiento para otros dispositivos tecnológicos, no existen en el SIGC, lo que genera inconsistencias en la aplicación del procedimiento. Cabe señalar que esta situación ya había sido observada como Oportunidad de Mejora en la auditoría del año anterior, por lo que su persistencia constituye una No Conformidad.	Se evidencian oportunidades de fortalecimiento en la documentación de los procedimientos de mantenimiento preventivo, dado que, aunque el mantenimiento de los equipos de cómputo se realiza conforme al instructivo IN-A-GT-05-01, este y los instructivos referenciados para otros dispositivos (IN-A-GT-05-02, IN-A-GT-05-03 e IN-A-GT-05-04) no están actualizados ni cargados en el SIGC, generando inconsistencias en la aplicación del procedimiento y afectando la trazabilidad.	Actualizar el instructivo IN-A-GT-05-01 y elaborar o revisar los instructivos faltantes (IN-A-GT-05-02, IN-A-GT-05-03 e IN-A-GT-05-04), remitiéndolos a la Oficina Asesora de Aseguramiento de la Calidad para su aprobación y cargue al SIGC, garantizando que toda la documentación respalde correctamente la ejecución del mantenimiento preventivo.	Contar con instructivos actualizados, completos y cargados en el SIGC, que respalden la correcta ejecución del mantenimiento preventivo de todos los equipos de cómputo y demás dispositivos tecnológicos conforme al procedimiento.	14/03/2026	14/07/2026	Profesional Universitario

PD-A-GT-05 numeral 5.6 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que el informe anual de mantenimiento 2025 no cumple con los requisitos establecidos, ya que no cuenta con la firma del responsable, y no existe evidencia de su entrega al Coordinador del área de Hardware y Comunicaciones. La falta de firma y de constancia de remisión afecta la validez del informe como soporte del mantenimiento realizado.	Se evidencian oportunidades de fortalecimiento en el proceso de entrega y registro de informes de mantenimiento, dado que, aunque el informe anual de mantenimiento 2025 se realiza y se socializa, no se cuenta con evidencia formal de su remisión al Coordinador del área de Hardware y Comunicaciones, y falta la firma del responsable, lo que afecta la validez del informe como soporte del mantenimiento realizado.	Realizar un seguimiento formal para la entrega y registro de los informes de mantenimiento anual, asegurando la firma del responsable y dejando evidencia documental de su remisión al Coordinador del área de Hardware y Comunicaciones, como complemento a la socialización verbal existente.	Contar con informe anual de mantenimiento debidamente firmado y con evidencia documental de su entrega al Coordinador del área de Hardware y Comunicaciones, garantizando la trazabilidad y validez del proceso, complementando la socialización verbal existente.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-06 numeral 6.2 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no existe un registro unificado, completo y trazable de las solicitudes correspondientes a la vigencia 2025, pese a que el procedimiento exige su gestión y control a través de la Mesa de Servicios. La información se encuentra fragmentada en distintos medios y la plataforma Chairá presenta limitaciones que impiden su adecuado seguimiento. Adicionalmente, esta situación ya había sido observada como Oportunidad de Mejora en la auditoría del año anterior.	Se evidencian oportunidades de fortalecimiento en el registro y control de las solicitudes gestionadas a través de la Mesa de Servicios, dado que no existe un registro unificado, completo y trazable correspondiente a la vigencia 2025. La información se encuentra fragmentada en distintos medios y la plataforma Chairá presenta limitaciones que impiden su adecuado seguimiento. Esta situación ya había sido observada como Oportunidad de Mejora en la auditoría del año anterior.	Implementar un mecanismo unificado para el registro, seguimiento y control de todas las solicitudes de la Mesa de Servicios, asegurando que la información sea completa, trazable y accesible, superando las limitaciones actuales de la plataforma Chairá.	Contar con un registro único, completo y trazable de todas las solicitudes gestionadas a través de la Mesa de Servicios para la vigencia 2025, que permita un seguimiento efectivo y cumpla con los requisitos del procedimiento establecido.	14/03/2026	14/07/2026	Profesional Universitario
Ley 1581 de 2012 Art 17 literal N Resolución 500 de 2021 Artículo 9 PD-A-GT-09 numeral 9.1 y 9.2 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no se están aplicando los pasos establecidos en el procedimiento de Gestión de Incidentes de Seguridad, a pesar de encontrarse vigente en el Sistema Integrado de Gestión de Calidad (SIGC). No se evidenció registro, diagnóstico, priorización, análisis, documentación, seguimiento, contención, generación de informes ni cierre formal de incidentes conforme a las actividades descritas en el procedimiento.	Se evidencian oportunidades de fortalecimiento en la aplicación del procedimiento de Gestión de Incidentes de Seguridad, dado que, aunque las actividades relacionadas con los incidentes se realizan, no se ejecutan conforme a los pasos establecidos en el procedimiento vigente en el SIGC, incluyendo registro, diagnóstico, priorización, análisis, documentación, seguimiento, contención, generación de informes y cierre formal de los incidentes.	Evaluar si se requiere actualización del procedimiento o en su defecto dar cumplimiento a las actividades conforme al procedimiento de gestión de incidentes de seguridad.	Garantizar que la gestión de incidentes de seguridad se ejecute conforme al procedimiento vigente.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-11 numerales 11.2 y 11.3 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no se están aplicando las actividades establecidas en el procedimiento de Gestión de Cambios de Tecnología de la Información, a pesar de encontrarse vigente en el Sistema Integrado de Gestión de Calidad. No existen registros del análisis de viabilidad del cambio, ni del establecimiento del impacto, ni de la aprobación del jefe de la OATI, etapas obligatorias para autorizar y planificar cualquier cambio.	Se evidencian oportunidades de fortalecimiento en la aplicación del procedimiento de Gestión de Cambios de Tecnología de la Información, dado que, aunque el procedimiento se encuentra vigente en el SIGC, no se están ejecutando todas las actividades obligatorias, como el análisis de viabilidad del cambio, la evaluación del impacto y la aprobación por el jefe de la OATI, etapas necesarias para autorizar y planificar correctamente cualquier cambio.	Asegurar la ejecución completa de todas las etapas establecidas en el procedimiento de Gestión de Cambios de Tecnología de la Información, incluyendo análisis de viabilidad, evaluación de impacto y aprobación por el jefe de la OATI, dejando registros documentales que respalden cada cambio realizado.	Contar con todos los cambios de Tecnología de la Información autorizados, planificados y documentados conforme al procedimiento vigente, garantizando análisis de viabilidad, evaluación de impacto y aprobación formal, asegurando trazabilidad y cumplimiento del SIGC.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-11 numerales 12.2 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	A fecha de la auditoría se evidenció que no se ha realizado la evaluación del cumplimiento de los objetivos establecidos en el PESPI para la vigencia 2025.	Se evidencian oportunidades de fortalecimiento en la evaluación del cumplimiento de los objetivos establecidos en el PESPI, dado que durante la auditoría no se ha realizado la evaluación correspondiente a la vigencia 2025, lo que limita la medición efectiva del desempeño y la trazabilidad del cumplimiento de metas institucionales.	Realizar la evaluación del cumplimiento de los objetivos establecidos en el PESPI para la vigencia 2025 y vigencias futuras, documentando los resultados y evidencias correspondientes conforme al procedimiento establecido.	Contar con la evaluación del cumplimiento de los objetivos del PESPI 2025 realizada, documentada y trazable, garantizando información confiable para la medición del desempeño institucional y la toma de decisiones.	14/03/2026	14/07/2026	Profesional Universitario

PD-A-GT-11 Numerales 12.5 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no se ha aplicado el instrumento de evaluación de controles del Modelo de Seguridad y Privacidad de la Información (MSPI), ni se ha documentado el estado actual de la seguridad de la información de la Universidad, pese a ser actividades obligatorias del procedimiento vigente para la elaboración del PESPI por vigencia.	Se evidencian oportunidades de fortalecimiento en la aplicación del procedimiento para la elaboración del PESPI, dado que no se ha aplicado el instrumento de evaluación de controles del Modelo de Seguridad y Privacidad de la Información (MSPI), ni se ha documentado el estado actual de la seguridad de la información de la Universidad, actividades obligatorias para la vigencia correspondiente.	Aplicar el instrumento de evaluación de controles del MSPI y documentar el estado actual de la seguridad de la información de la Universidad, asegurando que todas las actividades obligatorias del procedimiento vigente para la elaboración del PESPI se cumplan correctamente.	Contar con la evaluación de controles del MSPI aplicada y el estado de la seguridad de la información debidamente documentado, garantizando el cumplimiento del procedimiento vigente y la trazabilidad para la elaboración del PESPI por vigencia.	14/03/2026	14/07/2026	Profesional Universitario
PD-A-GT-15 numerales 15.5 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no existe registro de la comunicación con el usuario para agendar la fecha y hora de realización de las copias de seguridad, pese a que esta actividad está establecida en el procedimiento de Gestión de Copias de Seguridad. Esta situación ya había sido observada como oportunidad de mejora en la vigencia anterior.	Se evidencian oportunidades de fortalecimiento en el procedimiento de Gestión de Copias de Seguridad, dado que, aunque las copias de seguridad se realizan, el procedimiento vigente no establece claramente el registro formal de la comunicación con los usuarios para agendar la fecha y hora de realización, lo que limita la trazabilidad de la actividad.	Actualizar el procedimiento de Gestión de Copias de Seguridad para clarificar y formalizar el registro de la comunicación con los usuarios al agendar la realización de las copias, asegurando evidencia documental de cada programación.	Contar con un procedimiento actualizado y claro que respalde la realización de las copias de seguridad, incluyendo el registro formal de la comunicación con los usuarios, garantizando trazabilidad y cumplimiento del procedimiento.	14/03/2026	14/07/2026	Profesional Universitario
Ley 1581 de 2012 Art 4 literal G, Art 17 literal D PD-A-GT-15 numerales 15.9 ISO 9001:2015 e ISO 21001:2018 Requisito 7.5	Durante la auditoría se evidenció que no se encuentra documentado ningún paso del proceso realizado para las copias de seguridad, incumpliendo lo establecido en el procedimiento de Gestión de Copias de Seguridad.	Se evidencian oportunidades de fortalecimiento en la documentación del proceso de copias de seguridad, dado que no se encuentra registrado ningún paso realizado, incumpliendo lo establecido en el procedimiento vigente de Gestión de Copias de Seguridad.	Actualizar y aplicar el procedimiento de Gestión de Copias de Seguridad, asegurando que todos los pasos del proceso queden debidamente documentados y respaldados como evidencia.	Contar con registros completos y documentados de todas las actividades realizadas en el proceso de copias de seguridad, garantizando cumplimiento del procedimiento y trazabilidad de la información.	14/03/2026	14/07/2026	Profesional Universitario
ISO 9001:2015 e ISO 21001:2018 Requisito 7.5 Acuerdo No. 18 de 2017 Artículo 7	Durante la auditoría se evidenció que no se ha establecido la programación semestral exigida para la administración de las Salas de Cómputo, la cual debe incluir: 1. Mantenimiento preventivo de hardware y software, 2. Revisión de la configuración de conectividad, 3. Desinstalación de software sin licencia, 4. Redacción y entrega del informe final.	Se evidencian oportunidades de fortalecimiento en la gestión de las Salas de Cómputo, dado que no se ha establecido un procedimiento formal que contemple la programación semestral de mantenimiento preventivo de hardware y software, revisión de la configuración de conectividad, desinstalación de software sin licencia y redacción y entrega de los informes finales, lo que limita la trazabilidad y control de estas actividades.	Elaborar y aprobar un procedimiento formal de Gestión de Salas de Cómputo, que incluya la programación semestral de mantenimiento, revisión de conectividad, control de software y generación de informes, asegurando su aplicación y documentación para todas las salas.	Contar con un procedimiento formal y aprobado de Gestión de Salas de Cómputo que garantice la ejecución planificada de todas las actividades, incluyendo mantenimiento, revisión de conectividad, control de software y entrega de informes, asegurando trazabilidad y cumplimiento del control interno.	14/03/2026	14/07/2026	Profesional Universitario

Firma Reponsable del Proceso:

Nombre: Jairo Andres Durango Hernandez
Cargo: Coordinador Oficina Asesora de Tecnologias de la Información

Figura 5. Plan de mejoramiento auditoría de calidad proceso Gestión Tecnológica 2026.

Fuente: Elaboración propia.

7.2 ANEXO 2. REALIZACIÓN DE COPIAS DE SEGURIDAD 2026.

Casos en Mesa de Servicios

UNIVERSIDAD DE LA AMAZONIA

"Gestión e Investigación para el Desarrollo de la Amazonia"

Reporte Casos en Mesa de Servicios

COD	ESTAI	PRIORID	TRABAJ	TIPO	LUGAR	SOLICITAN	TERCERO	ERVICIO	DES ELEMEN	ELEMENT	DESCRIPCION	FECHAASIGNACI	FECHAFIN	DEPENDENCI	RESPONSABL	DOC RESPONSAB	FECHA CASO
23165	SOLUCIONADO	NORMAL	COPIA DE SEGURIDAD	SOLICITUD DE SERVICIO	OFICINA ASESORA TECNOLOGÍAS DE LA INFORMACIÓN	JAIRO ANDRES DURANGO HERNANDEZ	1117531360	ÁREA DE SISTEMAS	NO APLICA	NO APLICA	CORDIAL SALUDO, AMABLEMENTE SOLICITO SUBIR A LA NUBE Y VERIFICAR LAS COPIAS DE SEGURIDAD DE LAS BASES DE DATOS CHAIRÁ, SIIF, TFS Y MONGO DB, DEL MES DE ENERO. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	20/02/2026 08:49	09/04/2026 11:30	OFICINA ASESORA TECNOLOGÍAS DE LA INFORMACIÓN	PAOLA ANDREA RODRIGUEZ BETANCOURT	1117532097	20/02/2026 8:02
23207	SOLUCIONADO	NORMAL	COPIA DE SEGURIDAD	SOLICITUD DE SERVICIO	OFICINA ASESORA TECNOLOGÍAS DE LA INFORMACIÓN	JAIRO ANDRES DURANGO HERNANDEZ	1117531360	ÁREA DE SISTEMAS	NO APLICA	NO APLICA	CORDIAL SALUDO, AMABLEMENTE SOLICITO SUBIR A LA NUBE Y VERIFICAR LAS COPIAS DE SEGURIDAD DE LAS BASES DE DATOS CHAIRÁ, SIIF, TFS Y MONGO DB, DEL MES DE FEBRERO. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	09/04/2026 10:44	09/04/2026 11:30	OFICINA ASESORA TECNOLOGÍAS DE LA INFORMACIÓN	PAOLA ANDREA RODRIGUEZ BETANCOURT	1117532097	9/04/2026 10:04
23208	SOLUCIONADO	NORMAL	COPIA DE SEGURIDAD	SOLICITUD DE SERVICIO	OFICINA ASESORA TECNOLOGÍAS DE LA INFORMACIÓN	JAIRO ANDRES DURANGO HERNANDEZ	1117531360	ÁREA DE SISTEMAS	NO APLICA	NO APLICA	CORDIAL SALUDO, AMABLEMENTE SOLICITO SUBIR A LA NUBE Y VERIFICAR LAS COPIAS DE SEGURIDAD DE LAS BASES DE DATOS CHAIRÁ, SIIF, TFS Y MONGO DB, DEL MES DE MARZO. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	09/04/2026 10:45	09/04/2026 11:30	OFICINA ASESORA TECNOLOGÍAS DE LA INFORMACIÓN	PAOLA ANDREA RODRIGUEZ BETANCOURT	1117532097	9/04/2026 10:04

Figura 6. Realización de copias de seguridad 2026.

Fuente: Elaboración propia.