Universidad de la
Amazonia

Universidad de la Amazonia

Plan de Seguridad y Privacidad de la Información

2025

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 uno 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 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 de Tecnologías de la Información (OTI) 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 la misma (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 auditoria 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).

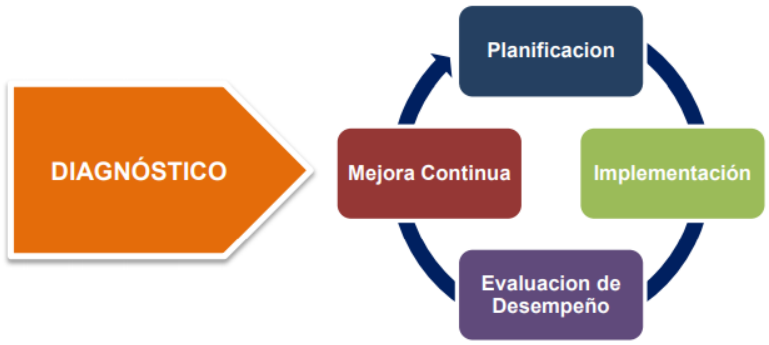

Figura 1. Fases del ciclo de operación del MSPI

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%

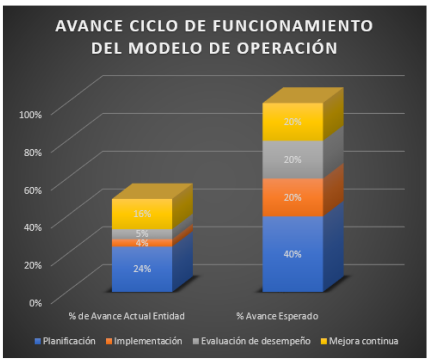

Figura 3. Avance de la implementación del modelo PHVA según la herramienta diagnóstico

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-y-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.pdf	
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 2025	
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%20017%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 Secretaría 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 Secretaría 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 sería 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		

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 2025 – Diciembre 2025
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). • Divulgación de la política de seguridad de la información.	OATI	Enero 2025 – Diciembre 2025

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 2025 – Diciembre 2025
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 2025 – Diciembre 2025
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 seguridad y privacidad de la información.	OATI	Enero 2025 – Diciembre 2025

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 2025 – Diciembre 2025
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 2025 – Diciembre 2025
Capacitaciones	• Ejecutar plan de mantenimiento de servicios tecnológicos. • Capacitar a los funcionarios administrativos en el uso de OneDrive institucional.	OATI	Enero 2025 – Diciembre 2025

Tabla 1. Planificación de actividades periodo enero 2025 – diciembre 2025

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 2025 – Diciembre 2025
Políticas de seguridad de la información	Divulgación de las políticas asociados a la política general de seguridad de la información.	OATI	Enero 2025 – Diciembre 2025
Roles y responsabilidades	Informe de revisión y actualización de roles y responsabilidades de los usuarios nuevos y antiguos.	OATI	Enero 2025 – Diciembre 2025
Activos de información	Documento de activos de información.	OATI	Enero 2025 – Diciembre 2025
Riesgos	• CoInforme de revisión y actualización de riesgos del proceso Gestión Tecnológica. • Informe de revisión y actualización del plan de tratamiento	OATI	Enero 2025 – Diciembre 2025

	de riesgos de seguridad de la información.		
Auditorías internas	Informe de resultados de auditoría de calidad.	Control Interno	Enero 2025 – Diciembre 2025
Copias de seguridad	Copias de seguridad subidas a la nube.	OATI	Enero 2025 – Diciembre 2025
Capacitaciones	Informe de personal capacitado en la Universidad.	OATI	Enero 2025 – Diciembre 2025

Tabla 2. Implementación y productos entregables según las actividades planeadas periodo enero 2025 – diciembre 2025.
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 2025 – Diciembre 2025
Políticas de seguridad de la información	Validación de la divulgación de las políticas asociadas a la política general de	OATI	Enero 2025 – Diciembre 2025

	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 2025 – Diciembre 2025
Activos de información	Documento aprobado de activos de información.	OATI	Enero 2025 – Diciembre 2025
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 2025 – Diciembre 2025
Auditorías internas	Plan de mejoramiento según el formato establecido por el SIGC.	OATI	Enero 2025 – Diciembre 2025

Copias de seguridad	Acta de verificación de las copias de seguridad subidas a la nube.	OATI	Enero 2025 – Diciembre 2025
Capacitaciones	Aprobación del informe de personal capacitado en la Universidad.	OATI	Enero 2025 – Diciembre 2025

Tabla 3. Evaluación de los productos entregables periodo enero 2025 – diciembre 2025

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 2025 – Diciembre 2025
Políticas de seguridad de la información	Revisión de limitaciones y observaciones según el informe presentado en la fase anterior.	OATI	Enero 2025 – Diciembre 2025
Roles y responsabilidades	Revisión de limitaciones y observaciones según el informe presentado en la fase anterior.	OATI	Enero 2025 – Diciembre 2025
Activos de información	Revisión de limitaciones y observaciones de la	OATI	Enero 2025 – Diciembre 2025

	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 2025 – Diciembre 2025
Auditorías internas	Revisión de los hallazgos de la auditoría realizada.	OATI	Enero 2025 – Diciembre 2025
Copias de seguridad	Revisión de limitaciones y observaciones de la realización de las copias de seguridad.	OATI	Enero 2025 – Diciembre 2025
Capacitaciones	Revisión de limitaciones y observaciones del personal no capacitado en la Universidad.	OATI	Enero 2025 – Diciembre 2025

Tabla 4. Mejora continua de los productos entregados periodo enero 2025 – diciembre 2025

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 2025-1

	FORMATO PLAN DE MEJORAMIENTO POR PROCESOS			
Universidad de la Amazonia	CÓDIGO: FO-E-GC-02-05	VERSIÓN: 5	FECHA: 10-01-2024	PÁGINA: 1 de 1

PROCESO:	Gestión Tecnologica
RESPONSABLE DEL PROCESO:	Jairo Andres Durango Hernandez
PERIODO AUDITADO:	Vigencia 2024 y 2025-1
FECHA DE SUSCRIPCIÓN	2/5/2025

CRITERIO	DESCRIPCIÓN DE LA NO CONFORMIDAD	ACCIÓN CORRECTIVA	META	FECHA DE INICIO	FECHA DE TERMINACION	RESPONSABLE ACCIÓN CORRECTIVA
Ley 594 de 2000 Acuerdo 42/2002 Consejo Directivo del Archivo General de la Nación. Norma ISO 9001:2015 Numerales 7.5.3 y 7.5.3.2 ISO 21001:2018 numeral 7.5.3, 7.5.3.2 GU-A-GD-01 guia de implementación de las tablas de retención documental.	No se evidencia archivo de gestión del proceso Gestión Tecnológica organizado cronologicamente, foliado, hoja de control y carpetas cuatro aletas de las vigencias anteriores.	Organizar el archivo del proceso de Gestión Tecnológica, según la guia de implementación de las tablas de retención documental GU-A-GD-01.	Disponer de un archivo organizado en carpetas, debidamente foliado.	2/5/2025	4/9/2025	Profesional Universitario
PD-S-AC-18 ISO 9001:2015 numeral 4.4.1 literal c y 8.5.1 y 7.5 ISO 21001:2018 numeral 4.4.1 literal c y 8.5.1 y 7.5	**Se evidencia incumplimiento dado que los siguientes indicadores presentan observaciones respecto a la medición y análisis de este.** **• Mesa de Servicios.** La fórmula matemática implementada en la matriz de evaluación a indicadores de gestión administrativa y académica (FO-S-AC-18-01) no coincide con la determinada en la caracterización del proceso. Adicional, no se tiene en cuenta las solicitudes atendidas mediante correo electrónico y comunicador interno institucional. **• Disponibilidad de la infraestructura tecnológica.** No se encuentra medido el segundo semestre de la vigencia 2024.	• Actualizar la fórmula matemática en la matriz de evaluación del indicador Mesa de Servicios y tener en cuenta las solicitudes atendidas mediante correo electrónico y comunicador interno institucional. • Realizar medición del indicador: Disponibilidad de la Infraestructura tecnológica 2024 y en los años siguientes.	• Disponer de una fórmula matemática en la matriz de evaluación del indicador Mesa de Servicios y adicionar la cantidad de solicitudes atendidas mediante correo electrónico y comunicador interno institucional. • Medir el indicador: Disponibilidad de la Infraestructura tecnológica 2024 y en los años siguientes.	2/5/2025	4/9/2025	Profesional Especializado
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 NTC - 9001:20015 7.5 ISO 21001:2018 Numeral 7.5	Se evidencia incumplimiento al Articulo 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 auditoria realizada a la vigencia 2022 se establece la NO conformidad, siendo	Se realizará el diagnóstico de la infraestructura para implementación de IPv6 y se solicitará al proveedor la entrega de las direcciones IPv6.	Garantizar la disponibilidad de infraestructura tecnológica apta para la implementación de IPv6, mediante la realización de un diagnóstico detallado y la solicitud ante el proveedor para que entregue de las direcciones IPv6 para culminar el proceso.	2/5/2025	4/9/2025	Profesional Universitario
ISO 9001:20015 8.1 literal d ISO 21001:2018 Numeral 8.1 Acuerdo No. 17 del 2017 (Política DTI) pagina 17	No existe evidencia del informe sobre la disponibilidad, confiabilidad y uso de los servicios ofrecidos, dando lugar a revisiones periódicas (una vez al año).	Diseñar y documentar un informe anual que evalúe la disponibilidad, confiabilidad y uso de los servicios ofrecidos por la OTI	Contar con un informe anual que evidencie la evaluación de la disponibilidad, confiabilidad y uso de los servicios ofrecidos, correspondiente al año en curso y los siguientes.	2/5/2025	4/9/2025	Profesional Universitario
PD-A-GT-01 ISO 9001:2015 ISO 21001:2018 Numeral 8.1	Se evidencia incumplimiento al objetivo registrado en el procedimiento para el mantenimiento preventivo de plataformas institucionales y de bases de datos, debido a que no existe planeación para el mismo en la vigencia 2024.	Planear y establecer un cronograma de mantenimiento preventivo, actividades técnicas, tiempos estimados de ejecución y registro de evidencias del cumplimiento.	Registro de evidencias del cumplimiento del mantenimiento preventivo a plataformas y sus respectivas actividades planificadas.	2/5/2025	4/9/2025	Profesional Universitario
PD-A-GT-01 Numeral 1.4 y 1.5 ISO 9001:2015 ISO 21001:2018 Numeral 7.5	No existe registro sobre el mantenimiento preventivo de plataformas institucionales y de bases de datos, que reporte las fechas y las actividades realizadas en el mantenimiento con recomendaciones, si las hubiere.	Registrar el mantenimiento preventivo de las plataformas institucionales y bases de datos a través del Módulo de Mesa de Servicios, como evidencia de la asignación del caso, incluyendo un cronograma de mantenimiento preventivo, actividades realizadas y las respectivas recomendaciones, si las hubiese.	Contar con un registro del mantenimiento preventivo de plataformas	2/5/2025	4/9/2025	Profesional Universitario
PD-A-GT-05 numeral 5.2 ISO 9001:2015 ISO 21001:2018 Numeral 7.5	No se llevó a cabo el registro del caso semestral en referencia a mantenimiento de los elementos tecnológicos en el Módulo de Mesa de Servicios en la plataforma.	Registrar caso semestral referente al mantenimiento de los elementos tecnológicos en el Módulo de Mesa de Servicios.	Disponer de un registro del caso semestral referente al mantenimiento de los elementos tecnológicos a través del Módulo de Mesa de Servicios.	2/5/2025	4/9/2025	Profesional Universitario

Figura 5. Plan de mejoramiento auditoría de calidad proceso Gestión Tecnológica 2025.

Fuente: Elaboración propia

7.2 ANEXO 2. CAPACITACIÓN ONEDRIVE

CAPACITACIÓN USO DE LA HERRAMIENTA ONEDRIVE

Nombre	Hora de entrada	Hora de salida	Correo electrónico	Rol
Jully Katerine Guzman Rodriguez	7/25/25, 3:17:05 PM	7/25/25, 4:26:17 PM	jull.guzman@udla.edu.co	Moderador
ANGIE PAOLA HERRERA RICARDO	7/25/25, 3:17:32 PM	7/25/25, 4:27:07 PM	ang.herrera@udla.edu.co	Moderador
OMAR ANDRES PENAGOS ASCENCIO	7/25/25, 3:18:04 PM	7/25/25, 4:19:25 PM	om.penagos@udla.edu.co	Moderador
GLORIA STEFANY ORTIZ SAENS	7/25/25, 3:19:42 PM	7/25/25, 4:20:15 PM	gl.ortiz@udla.edu.co	Moderador
LIGIA LOSADA LOSADA	7/25/25, 3:23:06 PM	7/25/25, 4:20:06 PM	li.losada@udla.edu.co	Moderador
Angie Viviana Checa Mendez	7/25/25, 3:27:29 PM	7/25/25, 4:20:25 PM	a.checa@udla.edu.co	Moderador
Keiny Fernanda Trujillo Quiroz	7/25/25, 3:28:48 PM	7/25/25, 4:29:48 PM	kei.trujillo@udla.edu.co	Moderador
DARLENSON QUINTO IBARGUEN	7/25/25, 3:28:49 PM	7/25/25, 4:21:38 PM	d.quinto@udla.edu.co	Moderador
SERGIO GOMEZ BARRERO	7/25/25, 3:30:05 PM	7/25/25, 3:43:19 PM	s.gomez@udla.edu.co	Moderador
PAOLA ANDREA RODRÍGUEZ BETANCOURT	7/25/25, 3:30:51 PM	7/25/25, 4:47:46 PM	p.rodriguez@udla.edu.co	Moderador
MILEYDI GUTIERREZ BASTIDAS (No comprobad	7/25/25, 3:31:06 PM	7/25/25, 4:23:04 PM		Moderador
MARTHA CECILIA PERDOMO CASALLAS	7/25/25, 3:31:12 PM	7/25/25, 4:22:27 PM	m.perdomo@udla.edu.co	Moderador
Fabián Andrés Cabrera Vargas	7/25/25, 3:31:26 PM	7/25/25, 4:19:46 PM		Moderador
WILDER ORLANDO MENESES GOMEZ	7/25/25, 3:31:32 PM	7/25/25, 4:22:42 PM	w.meneses@udla.edu.co	Moderador
Wilder Meneses DAC (No comprobado)	7/25/25, 3:32:09 PM	7/25/25, 4:21:53 PM		Moderador
Norma Constanza (No comprobado)	7/25/25, 3:32:48 PM	7/25/25, 4:19:36 PM		Moderador
Jhon Alexander Ipuz Niño	7/25/25, 3:33:35 PM	7/25/25, 4:20:14 PM	jh.ipuz@udla.edu.co	Moderador
Tatiana (No comprobado)	7/25/25, 3:33:40 PM	7/25/25, 3:33:48 PM		Moderador
Adela Hurtado Bustos (No comprobado)	7/25/25, 3:35:06 PM	7/25/25, 4:19:12 PM		Moderador
YESSICA ALEJANDRA SUAZA OBREGÓN	7/25/25, 3:35:26 PM	7/25/25, 4:06:23 PM	y.suaza@udla.edu.co	Moderador
ARBEY FABRIZIO MALAGON	7/25/25, 3:35:40 PM	7/25/25, 4:19:47 PM	a.malagon@udla.edu.co	Moderador
Jheison Arvey Garcia Moreno	7/25/25, 3:39:40 PM	7/25/25, 4:19:30 PM	jhei.garcia@udla.edu.co	Moderador
FABIO BELTRAN (No comprobado)	7/25/25, 3:41:08 PM	7/25/25, 4:47:46 PM		Moderador
MAYRA ALEJANDRA CÓRDOBA BELTRÁN	7/25/25, 3:41:45 PM	7/25/25, 4:19:38 PM	may.cordoba@udla.edu.co	Moderador
Jose Alejandro Salcedo Hoyos	7/25/25, 3:42:04 PM	7/25/25, 3:50:51 PM	jos.salcedo@udla.edu.co	Moderador
FABIO BELTRAN PERDOMO	7/25/25, 3:43:42 PM	7/25/25, 4:24:56 PM	fa.beltran@udla.edu.co	Moderador
Natalia Cobaleda (No comprobado)	7/25/25, 3:44:01 PM	7/25/25, 3:58:26 PM		Moderador
LUZ STELLA SUÁREZ JARAMILLO	7/25/25, 3:49:54 PM	7/25/25, 4:28:24 PM	lu.suarez@udla.edu.co	Moderador
CRISTIAN HERNANDEZ GIL	7/25/25, 3:52:34 PM	7/25/25, 3:56:05 PM	cris.hernandez@udla.edu.co	Moderador
YOLANDA MILENA CASTILLO VARGAS	7/25/25, 4:29:06 PM	7/25/25, 4:39:00 PM	y.castillo@udla.edu.co	Moderador

Figura 6. Capacitación de OneDrive institucional realizada por Microsoft Teams 2025.

Fuente: Elaboración propia

7.3 ANEXO 3. REALIZACIÓN DE COPIAS DE SEGURIDAD 2025.

Casos en Mesa de Servicios
UNIVERSIDAD DE LA AMAZONIA
"Gestión e Investigación para el Desarrollo de la Amazonia"
2025/11/25 a la(s) 01:59:05 p.m.
Reporte Casos en Mesa de Servicios

COD	ESTADO	PRIORIDAD	TRABAJO	TIPO	SOLICITANTE	DESCRIPCION	FECHAASIGNACION	FECHAFIN	RESPONSABLE	FECHA CASO
22728	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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.	11/3/2025 16:06	16/06/2025 17:30	PAOLA ANDREA RODRIGUEZ BETANCOURT	11/3/2025 16:03
22729	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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.	11/03/2025 16:08	16/06/2025 18:00	PAOLA ANDREA RODRIGUEZ BETANCOURT	11/3/2025 16:03
22765	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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.	08/04/2025 16:17	16/06/2025 18:00	PAOLA ANDREA RODRIGUEZ BETANCOURT	8/4/2025 16:04
22827	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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 ABRIL. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	13/05/2025 15:29	16/06/2025 18:00	PAOLA ANDREA RODRIGUEZ BETANCOURT	13/5/2025 15:05
22848	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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 MAYO. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	03/06/2025 10:17	16/6/2025 18:00	PAOLA ANDREA RODRIGUEZ BETANCOURT	3/6/2025 10:06
22922	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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 JUNIO. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	29/07/2025 09:03	29/07/2025 18:00	PAOLA ANDREA RODRIGUEZ BETANCOURT	29/7/2025 09:07
22965	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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 JULIO. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	19/08/2025 17:31	20/08/2025 14:30	PAOLA ANDREA RODRIGUEZ BETANCOURT	19/8/2025 17:08
22990	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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 AGOSTO. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	02/09/2025 07:43	06/10/2025 18:00	PAOLA ANDREA RODRIGUEZ BETANCOURT	2/9/2025 07:09
23024	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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 SEPTIEMBRE. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	29/09/2025 09:52	06/10/2025 18:00	PAOLA ANDREA RODRIGUEZ BETANCOURT	29/9/2025 09:09
23086	ARCHIVADO	NORMAL	COPIA DE SEGURIDAD	GESTIÓN DE COPIAS DE SEGURIDAD	JAIRO ANDRES DURANGO HERNANDEZ	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 OCTUBRE. AGRADEZCO SU COLABORACIÓN Y PRONTA GESTIÓN.	10/11/2025 09:30	10/11/2025 17:30	PAOLA ANDREA RODRIGUEZ BETANCOURT	10/11/2025 09:11

Figura 7. Realización de copias de seguridad 2025.

Fuente: Elaboración propia