Universidad de la.
Amazonia

Universidad de la Amazonia

Plan de Seguridad y Privacidad de la Información

2024

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 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 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 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).

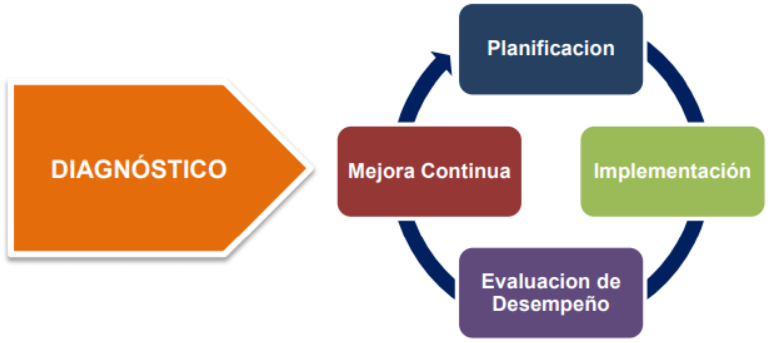

Figura 1. Fases del ciclo de operación del MSPI

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%

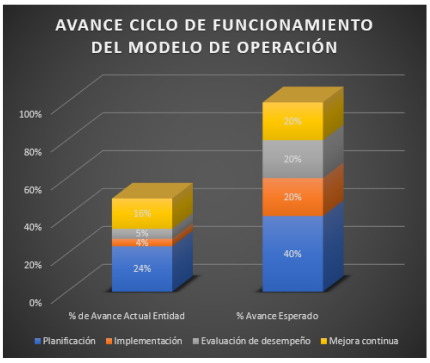

Figura 3. Avance de la implementación del modelo PHVA según la herramienta diagnóstico

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 BÁSICA 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	
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		
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/la-universidad/organigrama.html	
6	Políticas de seguridad de la información formalizada y firmada	http://www.uniamazonia.edu.co/documentos/docs/Consejo%20Superior/Acuerdos/2017/Acuerdo%20179%20Politicas%20del%20SGI.pdf	
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	http://www.uniamazonia.edu.co/documentos/docs/Consejo%20Superior/Acuerdos/2017/Acuerdo%20179%20Politicas%20del%20SGI.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		
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	Instrumento de evaluación 2020	
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%20de%20riesgo/01.F.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%20de%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%20179%20Politicas%20del%20SGI.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		
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		
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 auditorias 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.	http://www.uniamazonia.edu.co/documentos/docs/Consejo%20Superior/Acuerdos/2017/Acuerdo%20179%20Politicas%20del%20SGI.pdf	
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%20de%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		

	Porcentaje de cumplimiento del MSPI en los procesos de la entidad	# total de procesos	# de procesos definidos en el alcance	Total avance por procesos
43	Con base al alcance definido en la política de seguridad y el total de procesos de la	20	5	25%

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	• Actualización de la política de seguridad de la información (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.	OTI	Enero 2024 – Diciembre 2024
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.	OTI	Enero 2024 – Diciembre 2024
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	OTI	Enero 2024 – Diciembre 2024

	instalación de software (en caso de ser necesario).		
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.	OTI	Enero 2024 – Diciembre 2024
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.	OTI	Enero 2024 – Diciembre 2024
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	OTI	Enero 2024 – Diciembre 2024

	el módulo de Mesa de Servicios.		
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.	OTI	Enero 2024 – Diciembre 2024
Capacitaciones	• Ejecutar plan de mantenimiento de servicios tecnológicos. • Capacitar a los funcionarios administrativos en el uso de OneDrive institucional.	OTI	Enero 2024 – Diciembre 2024

Tabla 1. Planificación de actividades periodo enero 2024 – diciembre 2024

Fuente: Elaboración propia

6.3 FASE IMPLEMENTACIÓN

IMPLEMENTACIÓN			
Gestión	**Entregable(s)**	**Responsable**	**Fecha de ejecución**
Política de seguridad de la información	Informe de revisión, actualización y divulgación de la política de seguridad de la información.	OTI	Enero 2024 – Diciembre 2024
Políticas de seguridad de la información	Informe de revisión, actualización y divulgación de las políticas asociados a la	OTI	Enero 2024 – Diciembre 2024

	política general de seguridad de la información.		
Roles y responsabilidades	Informe de revisión y actualización de roles y responsabilidades de los usuarios nuevos y antiguos.	OTI	Enero 2024 – Diciembre 2024
Activos de información	Documento de activos de información.	OTI	Enero 2024 – Diciembre 2024
Riesgos	• Informe de revisión y actualización de riesgos del proceso Gestión Tecnológica. • Informe de revisión y actualización del plan de tratamiento de riesgos de seguridad de la información.	OTI	Enero 2024 – Diciembre 2024
Auditorías internas	Informe de resultados de auditoría de calidad.	Control Interno	Enero 2024 – Diciembre 2024
Copias de seguridad	Copias de seguridad subidas a la nube.	OTI	Enero 2024 – Diciembre 2024
Capacitaciones	Informe de personal capacitado en la Universidad.	OTI	Enero 2024 – Diciembre 2024

Tabla 2. Implementación y productos entregables según las actividades planeadas periodo enero 2024 – diciembre 2024

Fuente: Elaboración propia

6.4 FASE EVALUACIÓN

EVALUACIÓN			
Gestión	**Resultado(s)**	**Responsable**	**Fecha de ejecución**
Política de seguridad de la información	Aprobación del informe de revisión, actualización y divulgación de la política de seguridad de la información.	OTI	Enero 2024 – Diciembre 2024
Políticas de seguridad de la información	Aprobación del informe de revisión, actualización y divulgación de las políticas asociadas a la política general de seguridad de la información.	OTI	Enero 2024 – Diciembre 2024
Roles y responsabilidades	Aprobación del informe de revisión y actualización de roles y responsabilidades de los usuarios nuevos y antiguos.	OTI	Enero 2024 – Diciembre 2024
Activos de información	Documento aprobado de activos de información.	OTI	Enero 2024 – Diciembre 2024

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.	OTI	Enero 2024 – Diciembre 2024
Auditorías internas	Plan de mejoramiento según el formato establecido por el SIGC.	OTI	Enero 2024 – Diciembre 2024
Copias de seguridad	Acta de verificación de las copias de seguridad subidas a la nube.	OTI	Enero 2024 – Diciembre 2024
Capacitaciones	Aprobación del informe de personal capacitado en la Universidad.	OTI	Enero 2024 – Diciembre 2024

Tabla 3. Evaluación de los productos entregables periodo enero 2024 – diciembre 2024

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.	OTI	Enero 2024 – Diciembre 2024
Políticas de seguridad de la información	Revisión de limitaciones y observaciones según el informe presentado en la fase anterior.	OTI	Enero 2024 – Diciembre 2024
Roles y responsabilidades	Revisión de limitaciones y observaciones según el informe presentado en la fase anterior.	OTI	Enero 2024 – Diciembre 2024
Activos de información	Revisión de limitaciones y observaciones de la elaboración del documento de activos de información.	OTI	Enero 2024 – Diciembre 2024
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.	OTI	Enero 2024 – Diciembre 2024
Auditorías internas	Revisión de los hallazgos de la auditoría realizada.	OTI	Enero 2024 – Diciembre 2024

Copias de seguridad	Revisión de limitaciones y observaciones de la realización de las copias de seguridad.	OTI	Enero 2024 – Diciembre 2024
Capacitaciones	Revisión de limitaciones y observaciones del personal no capacitado en la Universidad.	OTI	Enero 2024 – Diciembre 2024

Tabla 4. Mejora continua de los productos entregados periodo enero 2024 – diciembre 2024

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 2024

Universidad de la Amazonia	FORMATO PLAN DE MEJORAMIENTO POR PROCESOS			
	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:	2023
FECHA DE SUSCRIPCIÓN	30/4/2024

CRITERIO	DESCRIPCIÓN DE LA NO CONFORMIDAD	ACCIÓN CORRECTIVA	META	FECHA DE INICIO	FECHA DE TERMINACION	RESPONSABLE ACCIÓN CORRECTIVA
No conformidad	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.	Se realizara la primera fase de transición al protocolo IPv6 correspondiente al diagnostico. .	Informe diagnóstico de transición del protocolo IPv4 a IPv6 según lo establecido por MinTIC.	6/5/2024	6/8/2024	Profesional Especializado
No conformidad	Al momento de la auditoria no se encontró diligenciado el Formato de Historia de Usuario (FO-A-GT-02-01) establecido para la toma y recolección de requisitos para el módulo liquidaciones desarrollado durante la vigencia 2023.	Se diligenciará el formato de Historia de Usuario (FO-A-GT-02-01) establecido para la toma y recolección de requisitos para el módulo liquidaciones y los siguientes módulos próximos a desarrollarse.	Historia de Usuario (FO-A-GT-02-01) diligenciada relacionada con el módulo de liquidaciones y proximos módulos a ser desarrollaldos.	6/5/2024	6/8/2024	Profesional Universitario
No conformidad	No se diligenció el formato de pruebas de software (FO-A-GT-02-02) para el desarrollo del módulo de Liquidaciones.	Se diligenciará el formato de pruebas de software (FO-A-GT-02-02) para el desarrollo del módulo de Liquidaciones y los siguientes módulos próximos a desarrollarse.	Prueba de Software (FO-A-GT-02-02 diligenciada relacionada con el módulo de liquidaciones y proximos módulos a ser desarrollaldos.	6/5/2024	6/8/2024	Profesional Universitario
No conformidad	No se evidencia formato de solicitud para la creación del procedimiento para el mantenimiento preventivo de plataformas institucionales y de bases de datos (PD- AGT-01)	Se diligenciará el formato de solicitud para la creación de los procedimientos futuros.	Formato de solicitud diligenciado solicitando para la creación de nuevos procedimientos.	6/5/2024	6/8/2024	Profesional Universitario

Figura 5. Plan de mejoramiento auditoría de calidad proceso Gestión Tecnológica 2024.

Fuente: Elaboración propia

7.2 ANEXO 2. CAPACITACIÓN ONEDRIVE

ASISTENTES A CAPACITACIÓN DE ONDRIVE 2024

ID	Hora de Inicio	Hora de finalizació	Correo electrónico	Numero de Docun	Nombre Completo	Dependencia	Cargo	¿Cómo valoraría su satisfacción general de la capa
1	11/15/24 14:32:02	11/15/24 14:32:32	anonymous	1004158456	Juan Jose Ortiz Plaza	OTI	Técnico Administrativo	5
2	11/15/24 14:32:09	11/15/24 14:32:42	anonymous	1117544883	Jheison Arvey Garcia Moreno	OTI	Técnico administrativo	5
3	11/15/24 14:33:03	11/15/24 14:33:27	anonymous	1094838704	Mario andres orozco sanchez	OTI	PROFESIONAL ADMINISTRAT	5
4	11/15/24 14:33:58	11/15/24 14:34:41	anonymous	40778442	RUBY SANCHEZ SANCHEZ	OIRI	PROFESIONAL UNIVERSITAR	5
5	11/15/24 14:34:36	11/15/24 14:35:07	anonymous	1006501224	Monica Moncada Conde	Programa Ingeniería de Alimentos	Oficinista	5
6	11/15/24 14:34:40	11/15/24 14:35:25	anonymous	52147395	Nathalie Sánchez Araujo	Coordinación Sede Leticia	Coordinadora Sede Leticia	3
7	11/15/24 14:35:10	11/15/24 14:35:58	anonymous	30393625	Claudia jimenez Arenas	Programa Ingeniería de Alimentos	Docente	4
8	11/15/24 14:35:24	11/15/24 14:36:09	anonymous	1117886099	ALEXANDER CUELLAR MURCIA	OTI	ASISTENTE	2
9	11/15/24 14:33:14	11/15/24 14:36:27	anonymous	1006514195	Cesar Augusto Obregon Sanchez	Oficina Tecnologías de la Información	Profesional Universitario	5
10	11/15/24 14:36:18	11/15/24 14:36:56	anonymous	1117499132	SANDRA MILENA SAPUY SILVA	DIRECCIÓN GESTIÓN TALENTO HUMANO	PROFESIONAL UNIVERSITAR	5
11	11/15/24 14:36:09	11/15/24 14:37:10	anonymous	1117539824	YOAN STEINER HUACA VALDES	OFICINA DE TECNOLOGIAS DE LA INFORM	PROFESIONAL UNIVERSITAR	5
12	11/15/24 14:36:06	11/15/24 14:37:27	anonymous	1117532097	Paola Andrea Rodriguez Betancourt	OTI	Profesional Especializado	5
13	11/15/24 14:36:55	11/15/24 14:37:39	anonymous	40778579	Sandra Patricia Díaz Jiménez	Liquidaciones	Coordinadora Oficina	5
14	11/15/24 14:36:59	11/15/24 14:37:51	anonymous	40611983	Yuly Palomares Suarez	Talento Humano	Técnico Administrativo	4
15	11/15/24 14:36:45	11/15/24 14:37:52	anonymous	1117508919	JONATHAN ANDRES ALBA ORTIZ	OTI	TECNICO ADMINISTRATIVO	5
16	11/15/24 14:36:09	11/15/24 14:38:17	anonymous	1117535553	MARIA ALEJANDRA TOLEDO HURT/	OIRI	PROFESIONAL UNIVERSITAR	3
17	11/15/24 14:37:24	11/15/24 14:38:43	anonymous	40760573	MARIA LUZ JARAMILLO SILVA	LICENCIATURA EN MATEMATICAS	OFICINISTA	4
18	11/15/24 14:38:27	11/15/24 14:39:10	anonymous	1117514828	Luz Stella Suárez Jaramillo	Oficina tecnologías de la información	Profesional universitario	4
19	11/15/24 14:48:23	11/15/24 14:49:23	anonymous	1006514021	Juddy Tatiana Vargas Santofimio	OTI	Auxiliar de salas	5
20	11/15/24 14:48:25	11/15/24 14:49:29	anonymous	1117542988	Danny Adrian Marles Muñoz	OTI	Profesional Universitario	5

Figura 6. Capacitación de OneDrive institucional realizada por Microsoft Teams 2024.

Fuente: Elaboración propia

7.3 ANEXO 3. REALIZACIÓN DE COPIAS DE SEGURIDAD 2024.

Casos en Mesa de Servicios
UNIVERSIDAD DE LA AMAZONIA
"Gestión e Investigación para el Desarrollo de la Amazonia"
2025/01/15 a la(s) 03:49:12 p.m.
Reporte Casos en Mesa de Servicios

CO	ESTADO	PRIORIDA	AREA	LUGAR	SOLICITANTE	DESCRIPCION	DEPENDENCIA	RESPONSABLE	FECHA CAS
21841	ARCHIVADO	NORMAL	SOFTWARE	OFICINA CONTROL INTERNO DISCIPLINARIO	ANGIE PAOLA HERRERA RICARDO	SOLICITUD DE HABILITACION DE ACCESO PARA ENVIAR CORREOS A FUI	OFICINA CONTROL INTERNO DISCIPLINARIO	YHEFFERSON ESNEIDER HUACA NUÑEZ	2/4/2024 14:04
21859	ARCHIVADO	NORMAL	SOFTWARE	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	LUZ STELLA SUAREZ JARAMILLO	Buenas tardes, es tan amable por favor eliminar el correo clau.cu	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 10:58
21865	ARCHIVADO	NORMAL	SOFTWARE	PROGRAMA DE INGENIERÍA DE ALIMENTOS	MAYRA ALEJANDRA CALDERON GIR	Buenas días. Con el propósito de generar actividades entre los gr	PROGRAMA DE INGENIERÍA DE ALIMENTOS	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 10:58
21894	ARCHIVADO	NORMAL	SOFTWARE	OFICINA ASESORA DE PLANEACIÓN	LUZ ANGELA NIETO SUAREZ	Buenas tardes, Solicito su valiosa colaboración verificando inforn	OFICINA ASESORA DE PLANEACIÓN	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 10:58
21896	ARCHIVADO	NORMAL	SOFTWARE	DESPACHO DPTO DE MEDIOS AUDIOVISUALES- CAMPUS CENT	LEONARDO ZAMORA VIVAS	En atención al asunto de la referencia, comedidamente solicito a	DESPACHO DPTO DE MEDIOS AUDIOVISUALES- CAMP	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 10:58
21909	ARCHIVADO	NORMAL	SOFTWARE	DIRECCION GESTION TALENTO HUMANO	DANIEL HERNANDEZ TRUJILLO	Fraternal saludo, De manera atenta y respetuosa, solicito la colat	DIRECCION GESTION TALENTO HUMANO	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 10:58
21924	ARCHIVADO	NORMAL	SOFTWARE	OFICINA DE EGRESADOS	JULY PAOLA RODRIGUEZ GAMEZ	Cordial Saludo,De manera respetuosa, me permito solicitar de su	OFICINA DE EGRESADOS	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 10:58
21926	ARCHIVADO	NORMAL	SOFTWARE	PROGRAMA DE ADMINISTRACIÓN FINANCIERA A DISTANCIA	NANCY OLAYA DELGADO	Atento saludo, Apreciados IngenierosDe manera cordial me permi	PROGRAMA DE ADMINISTRACIÓN FINANCIERA A DIST	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 10:58
21927	ARCHIVADO	NORMAL	SOFTWARE	OFICINA GESTIÓN DE INFORMACIÓN Y COMUNICACIÓN	STEFANIA RAMIREZ HOYOS	Respetado coordinador, buenas tardes. Amablemente me permito	OFICINA GESTIÓN DE INFORMACIÓN Y COMUNICACIÓ	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 10:58
21942	ARCHIVADO	NORMAL	SOFTWARE	ESPECIALIZACIÓN EN CONTROL INTERNO Y ASEGURAMIENTO	CHARYK TATIANA RIVAS MELO	Buenos días, es para solicitar el apoyo de ustedes para asignarle	ESPECIALIZACIÓN EN CONTROL INTERNO Y ASEGURAN	YHEFFERSON ESNEIDER HUACA NUÑEZ	17/4/2024 11:27
21958	ARCHIVADO	NORMAL	SOFTWARE	SECCIÓN DE CONTABILIDAD	CAROLINA BASTO TRUJILLO	Buenos días Ingeniero, solicito su apoyo en el sentido de poder a	SECCIÓN DE CONTABILIDAD	YHEFFERSON ESNEIDER HUACA NUÑEZ	22/4/2024 08:05
21971	ARCHIVADO	NORMAL	SOFTWARE	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	LUZ STELLA SUAREZ JARAMILLO	Cordial saludo, amablemente solicito de su apoyo con asignar un	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	YHEFFERSON ESNEIDER HUACA NUÑEZ	22/4/2024 08:05
21995	ARCHIVADO	NORMAL	SOFTWARE	DIVISIÓN DE BIENESTAR UNIVERSITARIO	AUGUSTO EDUARDO GONZALEZ TOI	Cordial saludo, Adjunto texto de cabecera y pieza gráfica, para su r	DIVISIÓN DE BIENESTAR UNIVERSITARIO	YHEFFERSON ESNEIDER HUACA NUÑEZ	22/4/2024 08:05
22006	ARCHIVADO	NORMAL	SOFTWARE	OFICINA CONTROL INTERNO DISCIPLINARIO	ANGIE PAOLA HERRERA RICARDO	Cordialmente, Por medio del presente comedidamente solicito la	OFICINA CONTROL INTERNO DISCIPLINARIO	YHEFFERSON ESNEIDER HUACA NUÑEZ	22/4/2024 08:05
22010	ARCHIVADO	NORMAL	SOFTWARE	DIVISIÓN DE BIENESTAR UNIVERSITARIO	JOSE LUIS ZAPATA JIMENEZ	Cordial saludo, Comedida y respetuosamente me dirijo a ustedes,	DIVISIÓN DE BIENESTAR UNIVERSITARIO	YHEFFERSON ESNEIDER HUACA NUÑEZ	22/4/2024 08:05
22017	ARCHIVADO	NORMAL	SOFTWARE	PROGRAMA DE BIOLOGÍA	TARIN ALEXANDRA LUCERO GARZOI	Buen día, me permito solicitar a ustedes la creación de cuenta de	PROGRAMA DE BIOLOGÍA	YHEFFERSON ESNEIDER HUACA NUÑEZ	22/4/2024 08:05
22058	ARCHIVADO	NORMAL	SOFTWARE	HERBARIO	OSCAR MAURICIO LOPEZ FLORIANO	MANTENIMIENTO A LA RED DE INTERNET, YA QUE DESDE HACE UNAS S	HERBARIO	YHEFFERSON ESNEIDER HUACA NUÑEZ	3/5/2024 09:05
22078	ARCHIVADO	NORMAL	SOFTWARE	PROGRAMA DE QUÍMICA	ELKIN ALBERTO TILVEZ MARRUGO	EN EL ÚLTIMO MES SE VIENE PRESENTANDO FALLA EN EL SERVICIO DE	PROGRAMA DE QUÍMICA	YHEFFERSON ESNEIDER HUACA NUÑEZ	6/5/2024 01:05
22114	ARCHIVADO	NORMAL	SOFTWARE	DEPARTAMENTO DE EDUCACIÓN A DISTANCIA	DANNY ADRIAN MARLES MUÑOZ	Buen día, De acuerdo a la solicitud emanada por la jefe del área (	DEPARTAMENTO DE EDUCACIÓN A DISTANCIA	YHEFFERSON ESNEIDER HUACA NUÑEZ	9/5/2024 15:12
22133	ARCHIVADO	NORMAL	SOFTWARE	OFICINA INTERNACIONALIZACIÓN Y RELACIONES INTERINSTIT	SANDRA LILIANA ROJAS ALVAREZ	Cordial saludo, Estimados Ingenieros, Comedidamente solicito as	OFICINA INTERNACIONALIZACIÓN Y RELACIONES INTE	YHEFFERSON ESNEIDER HUACA NUÑEZ	9/5/2024 15:12
22140	ARCHIVADO	NORMAL	SOFTWARE	SECCIÓN DE CONTABILIDAD	CAROLINA BASTO TRUJILLO	Buenos días Ingeniero, solicito su apoyo en el sentido de concede	SECCIÓN DE CONTABILIDAD	YHEFFERSON ESNEIDER HUACA NUÑEZ	9/5/2024 15:12
22141	ARCHIVADO	NORMAL	SOFTWARE	DIVISIÓN DE BIENESTAR UNIVERSITARIO	DARLYN BOLAÑOS GARCIA	Cordial saludo, Respetuosamente desde la Dirección de Bienesta	DIVISIÓN DE BIENESTAR UNIVERSITARIO	YHEFFERSON ESNEIDER HUACA NUÑEZ	9/5/2024 15:12
22146	ARCHIVADO	NORMAL	SOFTWARE	PROGRAMA DE DERECHO	WILMER GIOVANNY TORRES MARQ	De manera respetuosa doy respuesta al correo que antecede info	PROGRAMA DE DERECHO	LUZ STELLA SUAREZ JARAMILLO	9/5/2024 15:12
22153	ARCHIVADO	NORMAL	SOFTWARE	VICERRECTORÍA ADMINISTRATIVA Y FINANCIERA	YISELA MENDEZ ROJAS	Cordial saludo,En atención al asunto de referencia, de manera at	VICERRECTORÍA ADMINISTRATIVA Y FINANCIERA	YHEFFERSON ESNEIDER HUACA NUÑEZ	9/5/2024 15:12

Figura 7. Realización de copias de seguridad 2024.

Fuente: Elaboración propia