Universidad de la Amazonia
Vigilada MinEducación

RESOLUCIÓN No. 2167
(06 de julio de 2023)

"Por el cual se establece, aprueba e implementa el Plan Estratégico de Seguridad y Privacidad de la Información (PESPI), vigencia 2023, de la Universidad de la Amazonia"

EL RECTOR DE LA UNIVERSIDAD DE LA AMAZONIA

En uso de sus atribuciones legales, constitucionales y en especial las que le confiere el artículo 69 de la Constitución Política, la Ley 30 de 1992[1], el artículo 32 del Acuerdo Superior No. 62 del 2002[2], y:

CONSIDERANDO QUE:

La Constitución Política de Colombia, en el artículo 69, garantiza la autonomía universitaria y consagra que las Universidades podrán darse sus directivas y regirse por sus propios estatutos, de acuerdo con la Ley.

La Ley 30 de 1992, en los artículos 28 y 29, ha precisado que la autonomía universitaria reconoce a las universidades el derecho a *"darse y modificar sus estatutos, designar sus autoridades académicas y administrativas, crear, organizar y desarrollar sus programas académicos, definir y organizar sus labores formativas, académicas, docentes, científicas y culturales, otorgar los títulos correspondientes, seleccionar a sus profesores, admitir a sus alumnos y adoptar sus correspondientes regímenes y establecer, arbitrar y aplicar sus recursos para el cumplimiento de su misión social y de su función institucional".*

El Acuerdo Superior No. 062 de 2002, establece el Estatuto General de la Universidad de la Amazonía, el cual consagra en el artículo 32 como funciones del Rector, entre otras: *"e) Implementar los sistemas de evaluación requeridos para la buena marcha institucional, mediante procedimientos y mecanismos ejecutados por las instancias respectivas, e informar de ello al Consejo Superior Universitario, f) Expedir los actos administrativos correspondientes; Adjudicar y suscribir los contratos que sean necesarios para el cumplimiento de los objetivos de la institución, atendiendo las disposiciones legales y estatutarias vigentes".*

Él Congreso de la República de Colombia expidió la Ley de Protección de Datos Personales mediante la Ley 1581 de 2012 con el objetivo de garantizar la privacidad y la protección de datos personales de los ciudadanos colombianos; esta legislación establece los principios, derechos y deberes que deben regir el tratamiento de la información personal, tanto en el sector público como en el privado.

El Acuerdo Superior No. 17 de 2017 *"Por el cual se adoptan las políticas del Departamento de Tecnologías de la Información de la Universidad de la Amazonia"*, establece las políticas operacionales encaminadas en la protección de la infraestructura tecnológica y mantenibilidad de los servicios de Tecnologías de la Información, garantizando la confidencialidad, integridad y

[1] *"Por la cual se organiza el servicio público de la Educación Superior".*
[2] *"Por el cual se deroga el Acuerdo 064 de 1993, y se adopta el Estatuto General de la Universidad de la Amazonia"*

Universidad de la Amazonia
Vigilada MinEducación

disponibilidad de los activos de información.

El Acuerdo Superior No. 18 de 2017 *"Por el cual se adopta el reglamento interno para la administración y uso de las salas de cómputo de la universidad de la amazonia"*, consagra los deberes y obligaciones de los docentes, estudiantes, administrativos y demás comunidad universitaria, y las normas para el uso, comportamiento y control de las salas de cómputo, las cuales se encuentran a disposición de toda la comunidad universitaria para realizar las actividades académicas, administrativas, de investigación, entre otras.

El Plan de Desarrollo Institucional 2020 – 2029 *"Gestión e Investigación para el Desarrollo de la Amazonia"* aprobado mediante el Acuerdo No. 43 de 2020 por parte del Consejo Superior Universitario de la Universidad de la Amazonia fijó mediante la línea "Eficiencia y excelencia administrativa", programa "Universidad Transparente", estrategia "Innovación Tecnológica", objetivo "3.26. Implementar política de protección de datos informáticos donde se detalle la seguridad de la información generada por el personal de la Universidad", para mejorar la seguridad y privacidad de los activos de información que la Universidad administra, gestiona y efectúa el tratamiento según lo regulado por MinTIC.

La Resolución No. 1519 de 2020 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones *"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"*, define los lineamientos para la correcta publicación y divulgación de los activos de información de las entidades, teniendo en cuenta los estándares de accesibilidad web, seguridad digital, datos abiertos, y demás condiciones técnicas.

La Resolución No. 500 de 2021 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"*, dispone que las entidades deben adoptar la estrategia de seguridad digital la cual debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), y estar articulada al habilitador "Seguridad y privacidad de la información" de la Política de Gobierno Digital de Colombia.

El Decreto No. 767 de 2022 expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*, indica que las entidades públicas en los términos del artículo 39 de la Ley 489 de 1998 están obligadas en definir, implementar y supervisar los lineamientos necesarios en seguridad y privacidad de la información para fortalecer la estrategia de seguridad digital adoptada por la entidad.

En virtud de lo anterior, se hace necesario establecer el Plan Estratégico de Seguridad y Privacidad de la Información en adelante (PESPI) de la Universidad de la Amazonia para la vigencia 2023 en aras de llevar a cabo la i) protección de la información sensible de la institución, ii) cumplir con las regulaciones y las leyes proferidas por el Ministerio de Tecnologías de la Información y las

Universidad de la Amazonia
Vigilada MinEducación

Comunicaciones, iii) prevención de incidentes de seguridad y iv) garantizar un apoyo para la gestión tecnología de la Alma Máter.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: ESTABLECER el Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) de la Universidad de la Amazonia para la vigencia 2023, como parte del proceso de apoyo Gestión Tecnológica, inscrito en el Sistema de Gestión de la Calidad con código PD-A-GT-12 "Procedimiento elaboración del Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) por vigencia".

ARTÍCULO SEGUNDO: APROBAR el Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) de la Universidad de la Amazonia para la vigencia 2023, a través de la presente Resolución.

ARTÍCULO TERCERO: IMPLEMENTAR el Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) de la Universidad de la Amazonia, para la vigencia 2023, según las actividades definidas en el cronograma de ejecución del plan adjunto.

ARTÍCULO CUARTO: RESPONSABLE DE LA EJECUCIÓN DEL PLAN. El coordinador de la Oficina Tecnologías de la Información (OTI) es el responsable de la correcta ejecución del plan relacionado en el PESPI. Asimismo, de actualizar el plan en las nuevas vigencias según los lineamientos actuales y nuevos referentes a la Política de Gobierno Digital de Colombia.

ARTÍCULO QUINTO: SEGUIMIENTO Y EVALUACIÓN. La Oficina Asesora de Control Interno será la dependencia encargada de realizar seguimiento y evaluación de la implementación del plan por medio de las auditorías internas de forma trimestral.

ARTÍCULO SEXTO: SOCIALIZACIÓN. El Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) será socializado a la comunidad universitaria por los medios de difusión institucionales.

ARTÍCULO SÉPTIMO: VIGENCIA. La presente Resolución rige a partir de la fecha de su expedición y publicación de conformidad con lo previsto en el Acuerdo Superior No. 16 de 2019.

PÚBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Florencia – Caquetá, a los seis (06) días del mes julio del año dos mil veintitrés (2023)

FABIO BURITICÁ BERMEO
Rector

Proyectó: Miguel Leonardo Sánchez Fajardo
Coordinador Oficina Tecnologías de la Información
Revisó: William David Grimaldo Sarmiento
Secretario General
Revisó: Mónica Tobon Núñez
Profesional Especializada

(PESPI)

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIVERSIDAD DE LA AMAZONIA

"Gestión e Investigación para el Desarrollo de la Amazonia"

OFICINA TECNOLOGÍAS DE LA INFORMACIÓN

FLORENCIA - CAQUETÁ

2023

HISTORIAL DE CAMBIOS

No. VERSIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO DEL CAMBIO	FECHA
1	Elaboración del Documento	No Aplica	21-06-2023

TABLA DE CONTENIDO

CONTENIDO DE FIGURAS

CONTENIDO DE TABLAS

1. INTRODUCCIÓN.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en aras de proveer los lineamientos, directrices, guías, procedimientos y buenas prácticas, necesarias para fortalecer los mecanismos, estrategias y controles de seguridad y privacidad de la información para las empresas[1] públicas o sujetos obligados; mediante Decreto 767 de 2022 *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*, en su numeral "3.2. Seguridad y Privacidad de la Información" del Artículo 2.2.9.1.2.1. del Decreto mencionado; busca la implementación de los lineamientos de seguridad y privacidad de la información mediante la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual tiene como objetivo establecer la ruta de la estrategia de seguridad digital en las organizaciones para mantener, asegurar, respaldar, supervisar y monitorear la infraestructura tecnológica, servicios TI y demás activos de información, importantes para el funcionamiento de los procesos misionales y estratégicos.

Asimismo, la Resolución 500 de 2021 *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"*, exige a los sujetos obligados la implementación de controles para garantizar las operaciones seguras de las infraestructuras críticas, resiliencia y continuidad del negocio, interoperabilidad con los procesos, mecanismos de autenticación, proceso de desarrollo de software seguro, incidentes de seguridad, y demás establecidos en el Anexo A de la norma ISO/IEC 27001:2013. En ese sentido, la Universidad de la Amazonia, a través de la Oficina Tecnologías de la Información, órgano asesor que complementa y fortalece los procesos misionales de la Universidad de la Amazonia mediante la implementación, sistematización y mejora continua de los procedimientos y actividades mediante las Tecnologías de la Información y las Comunicaciones (TIC), elabora el presente plan para dar cumplimiento a lo exigido por MinTIC y ejecutar las fases del MSPI para la creación del SGSI con sus respectivos procedimientos relacionados.

[1] También denominadas organizaciones, entidades, instituciones, etc.

2. OBJETIVOS.

2.1 GENERAL.

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Universidad de la Amazonia, para reducir los riesgos informáticos a los que está expuesta la institución hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este plan para la vigencia 2023.

2.2 ESPECÍFICOS.

- Definir y establecer la estrategia de seguridad digital de la Universidad.
- Priorizar los proyectos de las estrategias específicas para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del SGSI.

3. ALCANCE.

El presente plan tendrá en cuenta todos los procesos de la Universidad de la Amazonia para la ejecución de los proyectos de las estrategias específicas definidas en el apartado 6.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES.

4. DOCUMENTOS DE REFERENCIA.

PESPI se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

Ley 23 de 1982 *"Sobre derechos de autor"*. Tiene como objetivo proteger la creación de las obras literarias, científicas y artísticas del creador/autor o coautores, en sus derechos de producción, difusión, transferencia, morales, entre otros.

Ley 527 de 1999 *"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"*. Tiene

como objetivo establecer los requisitos jurídicos para el uso, comunicación y conservación de los mensajes de texto; firmas digitales, certificados y entes certificadores para acreditar la veracidad de los datos contenidos en los mensajes de texto y certificados.

Ley 1032 de 2006. *"Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal"*. Establece los artículos:

- Artículo 257. Prestación, acceso o uso ilegal de los servicios de telecomunicaciones a través de la copia, reproducción, difusión y derivación, sin previa autorización.
- Artículo 271. Violación a los derechos patrimoniales por medio de reproducción, exhibición, alquiler, retransmisión y recepción de obras literarias, científicas o artísticas, sin previa autorización del autor.
- Artículo 272. Violación a los mecanismos de protección de derechos de autor y conexos, ya que suprima, altere, fabrique e importe, sin previa autorización del autor, las obras literarias, científicas o artísticas.
- Artículo 306. Usurpación de derechos de propiedad industrial y derechos de obtentores de variedades vegetales; utilizando sin previa autorización del autor, la marca o patente para favorecimiento económico y reputacional.

Ley 1221 de 2008 *"Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones"*. Tiene como objetivo establecer la normatividad necesaria para la implementación del teletrabajo en las empresas; instrumento para la generación y búsqueda de empleo mediante el uso de las TIC.

Ley 1266 de 2008 *"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"*. Tiene como objetivo disponer de la regulación pertinente sobre la actualización, rectificación, registro y conocimiento de los datos recogidos por las distintas fuentes de información, bancos de datos, entre

otros. Adicionalmente, otras normas relacionadas con el tratamiento de datos personales, a que se refiere el artículo 15 de la Constitución Política.

Ley 1273 de 2009 *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"*. Modifica el Código Penal agregando el tenor "CAPÍTULO I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", el cual protege los datos almacenados en los sistemas informáticos mediante los siguientes artículos:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva:
    - Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
    - Por servidor público en ejercicio de sus funciones.
    - Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
    - Revelando o dando a conocer el contenido de la información en perjuicio de otro.
    - Obteniendo provecho para sí o para un tercero.
    - Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
    - Utilizando como instrumento a un tercero de buena fe.

Ley 1341 de 2009 *"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"*. Tiene como objetivo regular, de manera general; la creación, implementación, supervisión y mejora continua de las políticas en el ámbito de las TIC, por ejemplo, la protección al usuario, calidad del servicio, inversión en el sector, usos eficientes de las telecomunicaciones, entre otras. También, posee 10 principios orientadores, los cuales promueven la aplicación correcta de las políticas anteriormente mencionadas; estos son:

- Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones.
- Libre competencia.
- Uso eficiente de la infraestructura y de los recursos escasos.
- Protección de los derechos de usuarios.
- Promoción de la inversión.
- Neutralidad tecnológica.
- El derecho a la comunicación, la información y la educación y los servicios básicos de las TIC.
- Masificación del Gobierno en Línea.
- Promoción de los contenidos multiplataforma de interés público.
- Acceso a las TIC y despliegue de infraestructura.

Ley 1581 de 2012 *"Por la cual se dictan disposiciones generales para la protección de datos personales"*. Tiene como objetivo establecer el régimen para la protección de datos personales. A diferencia de la Ley 1266 de 2008, el alcance se enfoca en el tratamiento de datos personales por el responsable del tratamiento o encargado del tratamiento. Asimismo, en la categorización de datos especiales (sensibles) recogidos, como origen racial o étnico, orientación política, convicciones religiosas, entre otras.

Ley 1712 de 2014 *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*. Tiene como

objetivo regular el acceso a la información pública por medio del derecho de acceso y principio de transparencia.

Decreto 415 de 2016 *"Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones"*. Establece los lineamientos TIC para el fortalecimiento de las entidades. A continuación, se mencionan algunos:

- Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado.
- Identificar oportunidades para adoptar nuevas tendencias tecnológicas que generen impacto en el desarrollo del sector y del País.
- Propender y facilitar el uso y apropiación de las tecnologías, los sistemas de información y los servicios digitales por parte de los servidores públicos, los ciudadanos y los grupos de interés a quienes están dirigidos.

Decreto 767 de 2022. *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".* Establece los lineamientos generales de la Política de Gobierno Digital, la cual es aplicable para los sujetos obligados de la administración pública en los términos del artículo 39 de la Ley 489 de 1998. Básicamente, la Política de Gobierno Digital de Colombia está estructurada en Habilitadores, como su nombre lo indica, habilitan las capacidades para cumplir con las Líneas de acción, estas permitirán la prestación de los servicios TI a la ciudadanía general de manera óptima, confiable y con los estándares de seguridad y privacidad de la información. Adicionalmente, comprende las Iniciativas

dinamizadoras, las cuales son proyectos de transformación digital que materializan dichas Líneas de acción.

Resolución 500 de 2021. *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"*. Establece los lineamientos necesarios para la implementación correcta del MSPI definiendo una estrategia de seguridad digital, la cual contendrá los roles y responsabilidades de seguridad y privacidad de la información en la entidad, efectuar el análisis y tratamiento de riesgos para la implementación de controles de seguridad, monitorear la infraestructura TI de amenazas del entorno o digitales para mantener las operaciones seguras, integrar los procesos organizacionales para tener un flujo de información interoperable, entre otros.

Política Nacional para la Transformación Digital e Inteligencia Artificial. Tiene como objetivo promover la adopción y desarrollo de tecnologías digitales e inteligencia artificial en el país, con el fin de impulsar la competitividad, mejorar la calidad de vida de los ciudadanos y fomentar la innovación en el sector público y privado, mediante la implementación de tecnologías 4RI. Además, resalta la importancia de la transformación digital, un motor de desarrollo económico y social, el cual establece una serie de lineamientos estratégicos para su implementación en el país, como la:

- Infraestructura digital: Mejora la cobertura y calidad de los servicios de telecomunicaciones promoviendo el uso de tecnologías como 5G e IoT.
- Gobierno digital: Fortalece la capacidad del Estado para ofrecer servicios digitales eficientes y transparentes a los ciudadanos.
- Economía digital: Impulsa la incorporación de las tecnologías 4RI para la creación de empleo en el sector digital.
- Seguridad digital: Fortalece la ciberseguridad y protección de datos en el país mediante la implementación de políticas y regulaciones.
- Inclusión digital: Busca el acceso equitativo a las tecnologías digitales e inteligencia artificial, especialmente en las zonas rurales y poblaciones vulnerables.

Política Nacional de Confianza y Seguridad Digital. Tiene como objetivo proporcionar medidas para la protección de datos, privacidad, integridad y disponibilidad de la información, con el fin de prevenir, mitigar y transferir el riesgo frente a las amenazas cibernéticas. Además, resalta la importancia de la seguridad digital en la sociedad actual, donde la digitalización y el uso de tecnologías digitales son cada vez más prominentes, ofreciendo una serie de lineamientos estratégicos para su implementación, como:

- Marco normativo y regulación: Fortalece el marco normativo y regulación en materia de seguridad digital, promoviendo la adopción de estándares y mejores prácticas internacionales.
- Gestión de riesgos cibernéticos: Gestiona la capacidad para identificar, evaluar y tratar los riesgos cibernéticos, mediante la implementación de políticas y medidas de seguridad adecuadas.
- Protección de datos personales: Garantiza la protección de datos personales, promoviendo el cumplimiento de las normas y regulaciones en materia de privacidad y protección de datos.
- Conciencia y cultura de seguridad digital: Promueve la concienciación de la seguridad digital en cualquier contexto, a través de programas de capacitación, educación y sensibilización.
- Cooperación nacional e internacional: Coopera entre diferentes entidades del Estado, sector privado, academia y sociedad civil, para para enfrentar las ciber amenazas.
- Innovación y desarrollo tecnológico seguro: Fomenta la innovación, desarrollo tecnológico, investigación y soluciones que incorporen medidas de seguridad.

5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Se utilizó el instrumento de evaluación de controles del MSPI, referenciado en la fase Diagnóstico (Análisis GAP) para conocer el estado actual de la seguridad y privacidad de la información de la Universidad de la Amazonia (ver Figura 1 y Figura 2).

Figura 1. *Evaluación de efectividad de controles según instrumento MSPI.*

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	42	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	31	100	REPETIBLE
A.9	CONTROL DE ACCESO	51	100	EFECTIVO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	51	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	63	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	54	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	63	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	69	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	54	100	EFECTIVO
A.18	CUMPLIMIENTO	47,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**49**	**100**	EFECTIVO

Fuente: Instrumento MSPI.

Figura 2. *Evaluación de efectividad de controles según instrumento MSPI.*

Fuente: Instrumento MSPI

En resumen, la Universidad de la Amazonia se encuentra en valoración Efectivo, es decir, algunos procesos se encuentran documentados y socializados, por ejemplo, plan de capacitación a docentes y funcionarios, a cargo de la Dirección Gestión Talento Humano; sin embargo, existen desviaciones en la implementación de controles o no es la forma correcta de aplicación, por ejemplo, difusión de la política de seguridad y privacidad de la información, políticas de control de acceso, relación con los proveedores y servicios tercerizados, entre otros. Claramente, la Universidad tiene que proyectar la hoja de ruta para mejorar la calificación actual, obtener un puntaje superior y determinar los recursos suficientes para la adopción del MSPI, MNGRSI y demás estrategias necesarias para garantizar la disponibilidad, integridad y confidencialidad de la información.

6. ESTRATEGIA DE SEGURIDAD DIGITAL.

La Universidad de la Amazonia establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del MSPI y MNGRSI. Por tal motivo, la Universidad de la Amazonia define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

Figura 3. *Estrategia de seguridad digital Uniamazonia.*

Fuente: Elaboración propia

6.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES).

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI, la Resolución 500 de 2021 y el Decreto 767 de 2022.

Tabla 1. *Estrategias específicas con su respectiva descripción.*

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Protección digital de los activos de información.	Adoptar el MSPI mediante aprobación de la alta dirección de las actividades enmarcadas en el PESPI para fortalecer la estrategia de seguridad digital de la Universidad de la Amazonia.
Gestión de riesgos TI y de corrupción.	Adoptar el MNGRSI para determinar los riesgos TI y de corrupción, alineados con el Sistema Integrado de Gestión de la Calidad de la Universidad de la Amazonia.
Capacitación seguridad TI.	Capacitar a la comunidad universitaria en seguridad de la información a partir de la ejecución del plan de capacitación institucional 2023-2025, FO-A-TH-05-04.
Gestión de incidentes de seguridad.	Implementar el procedimiento PD-A-GT-09 “PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD” ante la materialización de una amenaza y riesgo informático que afecte la disponibilidad, integridad y confidencialidad de los activos de información expuestos en el ciberespacio.

Fuente: Elaboración propia

6.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES.

Para cada estrategia específica, la Universidad de la Amazonia define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del SGSI:

Tabla 2. *Estrategias específicas con sus respectivos proyectos y productos esperados.*

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Protección digital de los activos de información.	Definición del alcance del MSPI.	Acto administrativo aprobado por la alta dirección donde se establezca el alcance del MSPI para la correcta adopción en la Universidad de la Amazonia.
	Definición de funciones de seguridad y privacidad de la información.	Acto administrativo aprobado por la alta dirección con las funciones de seguridad y privacidad de la información a los diferentes responsables.
	Definición de Roles y Responsabilidades de Seguridad de la Información.	Documento aprobado por la alta dirección donde se establecen los Roles y Responsabilidades de Seguridad de la Información.
Gestión de riesgos TI y de corrupción.	Actualización de la matriz de riesgos TI y corrupción del proceso Gestión Tecnológica teniendo en cuenta el MNGRSI.	Matriz de riesgos TI y corrupción actualizada del proceso Gestión Tecnológica.
Capacitación seguridad TI.	Adquisición de licencia de acceso a plataforma e-learning relacionada con las TIC.	Contrato de licenciamiento por 1 año en plataforma e-learning relacionada con las TIC.
Gestión de incidentes de seguridad.	Adquisición de dispositivos de seguridad perimetral para filtrado externo/interno de peticiones a los sistemas de información.	Instalación, configuración y puesta en funcionamiento de un NGFW.

Fuente: Elaboración propia

6.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS.

En la Tabla 3 se establece el cronograma de actividades de acuerdo con los proyectos asociados a los ejes de la estrategia de seguridad digital de la Universidad de la Amazonia. Asimismo, asignar los responsables y tiempo de ejecución para supervisar el cumplimiento de estas.

Tabla 3. *Cronograma de actividades según los proyectos definidos en el apartado 6.2.*

ESTRATEGIA / EJE	PROYECTO	RESPONSABLE	FECHA INICIO / FECHA FIN
Protección digital de los activos de información.	Definición del alcance del MSPI.	OTI.	Julio 2023 – Diciembre 2023.
	Definición de funciones de seguridad y privacidad de la información.	OTI.	Julio 2023 – Diciembre 2023.
	Definición de Roles y Responsabilidades de Seguridad de la Información.	OTI.	Julio 2023 – Diciembre 2023.
Gestión de riesgos TI y de corrupción.	Actualización de la matriz de riesgos TI y corrupción del proceso Gestión Tecnológica teniendo en cuenta el MNGRSI.	OTI.	Julio 2023 – Diciembre 2023.
Capacitación seguridad TI.	Adquisición de licencia de acceso a plataforma e-learning relacionada con las TIC.	OTI. Vicerrectoría Administrativa y Financiera.	Julio 2023 – Diciembre 2023.

Gestión de incidentes de seguridad.	Adquisición de dispositivos de seguridad perimetral para filtrado externo/interno de peticiones a los sistemas de información.	OTI.	Julio 2023 – Diciembre 2023.

Fuente: Elaboración propia

6.4 ANÁLISIS PRESUPUESTAL.

En la Tabla 4 se menciona el presupuesto asignado para la ejecución del cronograma de actividades definido en el apartado 6.3.

Tabla 4. *Análisis presupuestal de la ejecución del cronograma de actividades.*

ESTRATEGIA / EJE	PROYECTO	INVERSIÓN
Protección digital de los activos de información.	Definición del alcance del MSPI.	$0
	Definición de funciones de seguridad y privacidad de la información.	$0
	Definición de Roles y Responsabilidades de Seguridad de la Información.	$0
Gestión de riesgos TI y de corrupción.	Actualización de la matriz de riesgos TI y corrupción del proceso Gestión Tecnológica teniendo en cuenta el MNGRSI.	$0

Capacitación seguridad TI.	Adquisición de licencia de acceso a plataforma e-learning relacionada con las TIC.	$40.000.000 aprox.
Gestión de incidentes de seguridad.	Adquisición de dispositivos de seguridad perimetral para filtrado externo/interno de peticiones a los sistemas de información.	$400.000.000 aprox.

Fuente: Elaboración propia

7. RESPONSABLES

Representante legal de la Universidad de la Amazonia.

Coordinador Oficina Tecnologías de la Información.

Vicerrector(a) Administrativa y Financiera.

Demás dependencias asociadas a los procesos de la Universidad.

8. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento del Representante legal de la Universidad de la Amazonia con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.