Universidad de la
Amazonia

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2024

TABLA DE CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

1 INTRODUCCIÓN

“No existe una empresa 100% segura frente a la ciberdelincuencia y quien afirme eso, está engañando”, frase mencionada por José María Alonso Cebrián, conocido mundialmente como “Chema Alonso”, Chief Data Officer de Telefónica, en ESET Security Day en Valencia 2018. Lo anterior mencionado, es importante para las organizaciones, pues la implementación de dispositivos de seguridad (Firewall, IPS, IDS, Proxy, etc.), no garantiza la protección de los activos y la información siempre, ya que el riesgo, brechas de seguridad, desastres naturales, errores humanos, factores externos, entre otros, siempre está inmerso en cada estrategia de control de seguridad.

De esta manera, es primordial la ejecución periódica de la gestión de riesgos para identificar, analizar y tratar estos en cada uno de los procesos, por ende, es recomendable utilizar una metodología de análisis de riesgos informáticos que se ajuste a las necesidades de las organizaciones, ejemplo Magerit, Octave, Mehari, NIST SP 800 – 30, Cramm, etc. El resultado de la metodología permitirá detectar vulnerabilidades, amenazas, riesgos, brechas de seguridad, activos y demás, para adoptar medidas de control, protocolos de seguridad, software de seguridad y generar estrategias, políticas y procedimientos de seguridad de información.

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 Departamento de Tecnologías de la Información (DTI) 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 Tratamiento de Riesgos de Seguridad 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 definir responsabilidades y actividades para la verificación de riesgos asociados al proceso de Gestión Tecnológica en relación con el Acuerdo 09 de 2020 “Por el cual se adopta la Política de Administración de Riesgos de la Universidad de la Amazonia” y la Guía de Administración de Riesgos y Oportunidades de la Universidad de la Amazonia (GU-E-AC-11).

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Definir el plan de Tratamiento de Riesgos de Seguridad de la Información del proceso de Gestión Tecnológica en relación con el Acuerdo 09 de 2020 “Por el cual se adopta la Política de Administración de Riesgos de la Universidad de la Amazonia” y la Guía de Administración de Riesgos y Oportunidades de la Universidad de la Amazonia (GU-E-AC-11).

2.2 OBJETIVOS ESPECÍFICOS

- Revisar riesgos asociados al proceso Gestión Tecnológica del mapa de riesgos institucional de la Universidad de la Amazonia.

- Revisar grado de exposición inherente (riesgo sin controles) de los riesgos asociados al proceso Gestión Tecnológica.

- Revisar controles existentes, valoración del riesgo con controles y acciones de tratamientos de los riesgos asociados al proceso Gestión Tecnológica.

3 ALCANCE DEL DOCUMENTO

De acuerdo con las actividades a realizar dentro del plan de Tratamiento de Riesgos de Seguridad de la Información, el alcance de este documento corresponde a:

- Definición de riesgos, clasificación, grado de exposición, controles existentes, valoración del riesgo con controles y acciones de tratamiento del proceso Gestión Tecnológica.

- Asignación de responsabilidades a los funcionarios administrativos del Departamento de Tecnologías de la Información de la Universidad de la Amazonia.

4 GLOSARIO DE TÉRMINOS

- Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

- Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

- Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

- Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

- Consecuencia: Resultado de un evento que afecta los objetivos.

- Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

- Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

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

5 RESPONSABILIDAD

5.1 DEPARTAMENTO 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.

6 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

6.1 VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGOS DE LA UNIVERSIDAD DE LA AMAZONIA

El Departamento de Tecnologías de la Información asume la gestión de riesgos según el Acuerdo 09 de 2020 “Por el cual se adopta la Política de Administración de Riesgos de la Universidad de la Amazonia” y la guía de Administración de Riesgos y Oportunidades de la Universidad de la Amazonia (GU-E-AC-11). En la Figura 1 se observa la metodología utilizada para la administración de riesgos.

Figura 1. Modelo de Gestión de Riesgos de la Universidad de la Amazonia
Fuente: Universidad de la Amazonia

Sin embargo, los riesgos relacionados con seguridad de la información se encuentran vinculados en el proceso de Gestión Tecnológica. En ese sentido, este plan interviene en la fase de Identificación del Riesgo, Análisis del Riesgo y Valoración del Riesgo.

6.2 IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DEL RIESGO

De acuerdo con la guía GU-E-AC-11, se realizó el proceso de análisis de riesgo según la calificación del riesgo mencionada en esta (ver Tabla 1).

Impacto	Valor	Probabilidad	Valor
Leve	5	Baja	1
Moderado	10	Media	2
Fuerte	20	Alta	3

Tabla 1. Calificación del riesgo según la guía GU-E-AC-11

Fuente: Universidad de la Amazonia

Seguidamente, para la evaluación del riesgo se utilizó la matriz de calificación, evaluación y respuesta a los riesgos establecida en la misma guía (ver Tabla 2).

Probabilidad	Valor	Evaluación		
Alta	3	15 Zona de Riesgo Importante Evitar el Riesgo	30 Zona de Riesgo Inaceptable Reducir el Riesgo, Evitar, Compartir o Transferir	60 **Zona de Riesgo Inaceptable** Reducir el Riesgo, Evitar, Compartir o Transferir (En lo posible eliminar la actividad que lo genera)
Media	2	10	20	40

		Zona de Riesgo Moderado Asumir el Riesgo Reducir el Riesgo	Zona de Riesgo Importante Reducir el Riesgo, Evitar, Compartir o Transferir	Zona de Riesgo Inaceptable Reducir el Riesgo, Evitar, Compartir o Transferir
Baja	1	5 Zona de Riesgo Aceptable Asumir el Riesgo (Aceptarlo sin necesidad de tomar nuevas medidas de control)	10 Zona de Riesgo Moderador Reducir el Riesgo, Compartir o Transferir	20 Zona de Riesgo Importante Reducir el Riesgo, Compartir o Transferir
	Valor	5	10	20
	Impacto	**Leve**	**Moderado**	**Fuerte**

Tabla 2. Calificación, Evaluación y Respuesta a los riesgos según la guía GU-E-AC-11
Fuente: Universidad de la Amazonia

Finalmente, se elaboró la matriz de riesgos. A continuación, se muestra la verificación realizada durante el año 2024(ver Figura 2).

(1) PROCESO	(2) RIESGO	GRADO DE EXPOSICION INHERENTE	GRADO DE EXPOSICION RESIDUAL	CALIFICACION DE LA PROTECCION EXISTENTE		(14) ACCION DE TRATAMIENTO	(15) RESPONSABLE	(16) FECHA DE IMPLEMENTACION
				VALORACION	OPCION DE TRATAMIENTO			
GESTION TECNOLÓGICA	FALLAS DE HARDWARE	ZONA DE RIESGO INACEPTABLE	ZONA DE RIESGO MODERADO	Cambia la evaluación antes de controles	Reducir el riesgo	Mantenimiento y revisión al sistemas de respaldo (UPS)	Responsable del Proceso	31/12/2024
						Capacitación personal encargado	Responsable del Proceso	31/12/2024
						Dispositivos y elementos necesarios para el mantenimiento de infraestructura	Responsable del Proceso	31/12/2024
	PÉRDIDA DE LA INFORMACIÓN	ZONA DE RIESGO IMPORTANTE	ZONA DE RIESGO MODERADO	Cambia la evaluación antes de controles	Reducir el riesgo	Capacitación personal encargado	Responsable del Proceso	31/12/2024
						Procedimiento para realizar copias de seguridad	Responsable del Proceso	31/12/2024
						Sensibilización del uso adecuado de dispositivos de almacenamiento.	Responsable del Proceso	31/12/2024
	FALLAS DE SOFTWARE	ZONA DE RIESGO IMPORTANTE	ZONA DE RIESGO MODERADO	Cambia la evaluación antes de controles	Reducir el riesgo	Socializar instrutivos de uso de software.	Responsable del Proceso	31/12/2024
						Capacitación personal encargado	Responsable del Proceso	31/12/2024
						Adquisición (compra o desarrollo)	Responsable del Proceso	31/12/2024
	FALLAS DE REDES Y COMUNICACIONES	ZONA DE RIESGO INACEPTABLE	ZONA DE RIESGO MODERADO	Cambia la evaluación antes de controles	Reducir el riesgo	Capacitación personal encargado	Responsable del Proceso	31/12/2024
						Documentar el procedimiento	Responsable del Proceso	31/12/2024
						Mejoramiento de la infraestructura tecnológica	Responsable del Proceso	31/12/2024
	FALLAS DE SEGURIDAD	ZONA DE RIESGO INACEPTABLE	ZONA DE RIESGO IMPORTANTE	Cambia la evaluación antes de controles	Reducir el riesgo	Documentar el procedimiento	Responsable del Proceso	31/12/2024
						Capacitación personal encargado	Responsable del Proceso	31/12/2024
						Uso de software libre	Responsable del Proceso	31/12/2024
						Adquisición de dispositivos de seguridad	Responsable del Proceso	31/12/2024

Figura 2. Verificación de matriz de riesgos periodo 2024 Gestión Tecnológica

Fuente: Elaboración propia

6.3 LIMITACIONES DEL PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

- Falta de talento humano capacitado para realizar la revisión de la documentación.
- Ocurrencia de imprevistos ajenos en las fases del plan.