PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD

Universidad del Tolima

Oficina de Gestión Tecnológica

2022

OBJETIVO

Implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en la Universidad del Tolima con el fin de definir y

establecer controles sobre las amenazas, vulnerabilidades y riesgos, con el fin de mantener niveles de aceptación razonables de los mismos en relación con la disponibilidad, integridad y confidencialidad de la información institucional.

ALCANCE

El Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, que permita integrar en los procesos institucionales y la ejecución de buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos misionales, estratégicos, de formación y apoyo.

El presente plan tendrá en cuenta todos los riesgos identificados, brindando prioridad a de acuerdo a los niveles de mayor afectación, así como abarca los riesgos de menor impacto de acuerdo a las estrategias establecidas para mitigar los mismos-

MARCO NORMATIVO

- **Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1008 de 2018:** 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.
- **CONPES 3854 de 2016:** Política Nacional de Seguridad Digital
- **Manual para la Implementación de la Política de Gobierno Digital Implementación de la política de Gobierno Digital.** Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019 .
- **Resolución 500 de marzo 10 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.
- **Modelo de Seguridad y privacidad de la información** - MSPI Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

- **NTC / ISO 27001:2013:** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
- **NTC/ISO 31000:2009** Gestión del Riesgo. Principios y directrices.
- **Guía para la administración del riesgo y el diseño de controles en entidades públicas** – Versión 4 Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018
-

DEFINICIONES

- **Aceptación del riesgo:** Es el nivel máximo de riesgo que la entidad está dispuesta a aceptar**.**
- **Análisis del riesgo:** "Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel del riesgo", según NTC ISO 31000:2011.
- **Consecuencia:** Resultado o impacto de un evento que afecta a los objetivos.
- **Pérdida de la Confidencialidad:** Violación o incidente a la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.
- **Pérdida de la Integridad:** Pérdida de la propiedad de mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Pérdida de la Disponibilidad:** Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Seguridad de la Información:** Es el principio que busca crear condiciones de uso confiable del entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades, y de los servicios que prestan al ciudadano.
- **Riesgo:** Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera También se puede generar riesgo positivo

en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

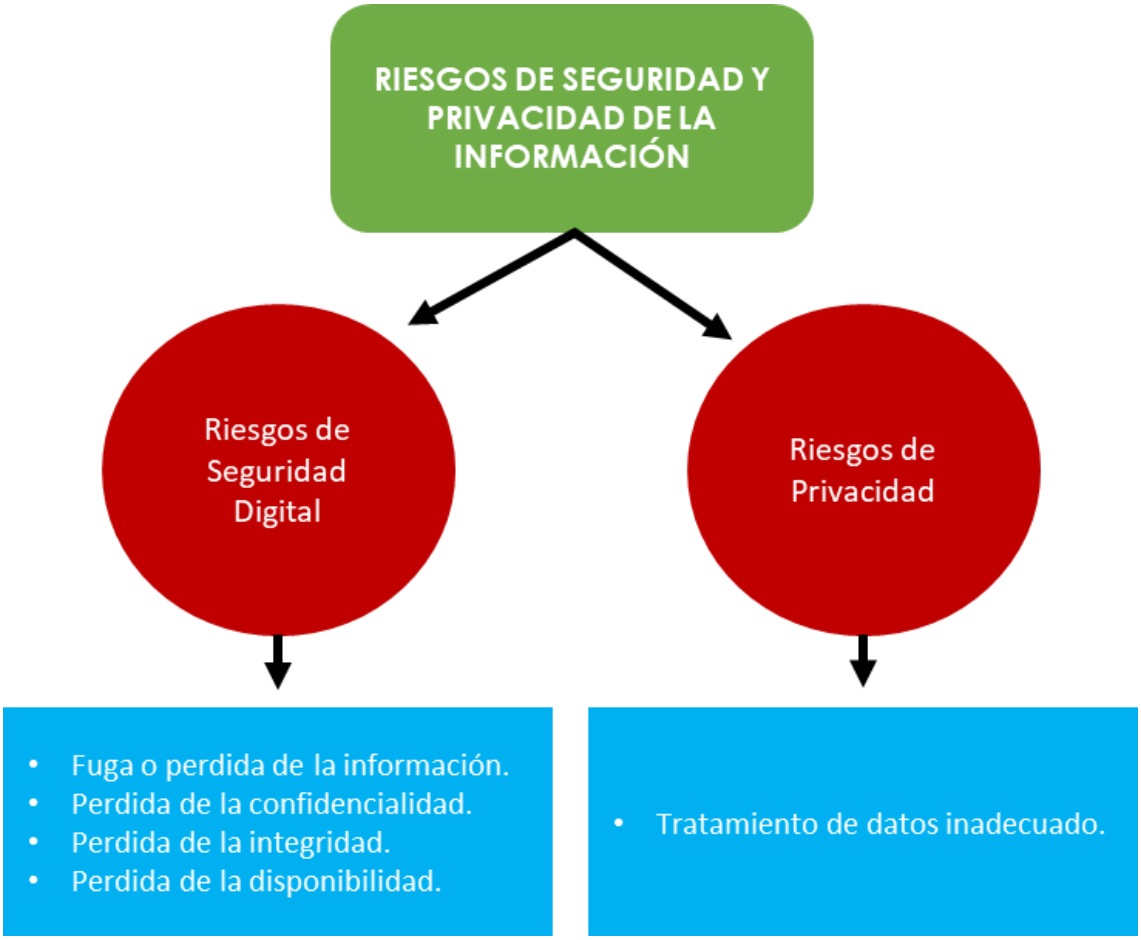
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

ESTRATEGÍA PARA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD

- Planificar: Establecer políticas, lineamientos , procesos y procedimientos que permitan identificar, analizar, y gestionar los riesgos y disminuir su impacto.
- Implementar: Ejecutar las acciones de acuerdo a las establecidas en la planificación con el fin de poder reducir el impacto y garantizar la continuidad de los procesos.
- Medir: Efectuar los respectivos seguimientos y evaluar los resultados de la estrategia a fin de establecer acciones de mejora.
- Mejorar: Tomar acciones correctivas, preventivas, basadas en los resultados para lograr una mejora continua.

DEFINICIÓN DEL RIESGO

Según la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "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". De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información. En el marco de la Política Nacional de Seguridad Digital, esta estratégia de tratamiento riesgos de la Universidad del Tolima busca identificar, gestionar y tratar los Riesgos de Seguridad y Privacidad de la Información, por lo que se reconocen los siguientes riesgos:



Criterios de evaluación de riesgos:

La evaluación de los riesgos de seguridad de la información se enfocará en:

- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones.

Criterios de Impacto:

Los criterios de impacto se determinará en términos del grado de afectación, daño y costo de reposición o reparación, causados por el evento de seguridad de la información y se considerará:

- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)

- Afectación de los grupos de interés.
- Afectación de la continuidad del servicio o proceso y el valor financiero.
- Implicación de los planes institucionales.
- Daños en la imagen institucional.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, clasificando y evaluando el evento con el fin de obtener información que identifique el nivel de afectación, permite su priorización y estrategia de tratamiento. Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

Probabilidad: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.

ESCALA DE PROBABILIDAD		
1	**Raro**	Evento que puede ocurrir sólo en circunstancias excepcionales, entre 0 y 1 vez en 1 semestre
2	**Improbable**	Evento que puede ocurrir en pocas de las circunstancias, entre 2 y 5 veces en un semestre.
3	**Posible**	Evento que puede ocurrir en algunas de las circunstancias entre seis y 10 veces en 1 semestre
4	**Probable**	Evento que puede ocurrir en casi siempre entre 11 y 15 veces en 1 semestre.
5	**Casi seguro**	Evento que puede ocurrir en la mayoría de las circunstancias más de 15 veces en 1 semestre.

Impacto: Hace referencia a las consecuencias que puede ocasionar a la Universidad la materialización del riesgo; se refiere a la magnitud de sus efectos.

ESTIMACIÓN DEL IMPACTO			Escala
1	**Insignificante**	Impacta negativamente de forma leve la imagen y operación de un rol. No tiene impacto Financiero para la Universidad o sus procesos.	1 a 4
2	**Menor**	Impacta negativamente la imagen y de manera importante la operación de un proceso. Se pueden presentar sobrecostos debido a reprocesos a nivel de un proceso.	5 a 8
3	**Moderado**	Afecta negativamente la imagen Institucional a nivel regional por retrasos en la prestación de los servicios y la operación no sólo del proceso evaluado sino de otros procesos. Se pueden presentar sobrecostos por reprocesos y aumento de carga operativa, no sólo en el proceso evaluado sino a otros procesos. Impacta negativamente, posibilidad de recibir una investigación disciplinaria.	9 a 12
4	**Mayor**	Imagen Institucional a nivel nacional afectada, al igual que la operación por el incumplimiento en la prestación de servicios de la Universidad o el cumplimiento de sus objetivos estratégicos o misionales. Se pueden presentar sobrecostos por reprocesos significativos para una sede seccional de la Institución. Impacta negativamente, posibilidad de recibir una investigación fiscal.	13 a 16
5	**Catastrófico**	Imagen Institucional afectada a nivel nacional e Internacional. Impacta negativamente la operación y el cumplimiento en la prestación de los servicios de la Institución y el incumplimiento de sus objetivos estratégicos misionales, estratégicos. Se pueden presentar sobrecostos debido a reprocesos y aumento de carga operativa importante en toda la Universidad. Impacta negativamente, posibilidad de recibir una intervención o sanción, por parte de entes de control o cualquier ente regulador.	17 a 20

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	META	PRODUCTO	FECHA
Análisis de Riesgos de Seguridad y Privacidad de la información	Identificar los riesgos de seguridad y privacidad	Matriz de tratamiento de riesgos de seguridad y privacidad	30/07/2022
	Establecer los criterios de evaluación e impacto		
Seguimiento y control de los Riesgos	Establecer las estratégicas de evaluación acuerdo a los eventos presentados y su nivel de criticidad-	Informe de tratamiento de riesgos	17/12/2022
Mejoramiento	Identificar las oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos.	Planes de mejoramiento	17/12/2022
Política de Seguridad y privacidad de la Información	Aprobación y publicación de la política por parte del Consejo Superior	Acuerdo por medio del cual se aprueba la política de seguridad y privacidad de la información para la Universidad del Tolima	30/04/2022