PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Universidad del Tolima

Oficina de Gestión Tecnológica

2024

INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información permite establecer las acciones necesarias y encaminadas a proteger, preservar y administrar la información de la Universidad del Tolima, emitida o gestionada a través de los diferentes medios tecnológicos a fin de asegurar su integridad, seguridad, legalidad y confidencialidad, garantizando el cumplimiento de los propósitos misionales, estratégicos, de formación y de apoyo de la institución.

El Plan de Seguridad y Privacidad de la Información de la Universidad del Tolima, está enfocada en adoptar los requerimientos y lineamientos establecidos en Gobierno Digital y Seguridad Digital, y lo dispuesto por la norma internacional ISO 27001, permitiendo tener una estratégica clara frente a la protección de los activos de la información.

OBJETIVO

Implementar el Plan de Seguridad y Privacidad de la Información en la Universidad del Tolima, como estrategia para la preservación, gestión y disponibilidad de la información institucional de acuerdo a las normativas y estándares nacionales e internacionales vigentes a los que aplique.

ALCANCE

Las Políticas de Seguridad y privacidad de la Información son aplicables para todos los procesos académicos, administrativos y de control de la Universidad del Tolima, quien es la encargada de facilitar los recursos humanos, técnicos, financieros y demás necesarios con el objetivo de dar cumplimiento y sostenibilidad a los activos de la información y su alcance aplica a todos los procesos misionales, estratégicos y de apoyo de la institución.

MARCO NORMATIVO

- 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.

- 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.
- 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.
- Ley 1581 de 2012, Principio de seguridad: "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente Ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."
- Ley 1581 de 2012, Artículo 17, ítem d: "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"
- Ley 1712 de 2014, "principio de transparencia": "Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta Ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la Ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta Ley."
- Decreto 1413 de 2017, "Seguridad de la información." "Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."

DEFINICIONES

- **Aceptación de riesgo:** Decisión de asumir un riesgo. Activo: Cualquier cosa que tiene valor para la organización.

Adaptabilidad: Define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

- **Amenazas:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.
- **Centros de cableado:** Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
- **Centro de cómputo:** Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos.
- **Ciberseguridad :** Capacidad del Estado para minimizar el nivel de riesgo aceptable al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Confiabilidad de la Información:** Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **Custodio del activo de información:** Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- **Datos personales:** Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.
- **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar

su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad.
- **Evaluación del riesgo**: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad**: Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Probabilidad:** es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Recursos informáticos:** Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de estos.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.
- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Tratamiento del riesgo**: Proceso de selección e implementación de acciones de mejora que permita gestionar el riesgo.
- **Valoración del riesgo**: Proceso de análisis y evaluación del riesgo.
- **Vulnerabilidad** : es una falencia o debilidad que puede estar

presente en la tecnología, las personas o en las políticas y procedimientos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	META	PRODUCTO	FECHA
Política de Seguridad y privacidad de la Información	* Viabilidad financiera de la política.	Acuerdo por medio del cual se aprueba la política de seguridad y privacidad de la información para la Universidad del Tolima	*29/02/2024
	* Entrega y aprobación del documento técnico. * Aprobación de la		*30/03/2024
	política ante el consejo superior.		*30/06/2024
Inventario de los Activos de la Información	* Verificación y/o corrección de la Matriz.	Documentos matriz de los activos de la información	* 30/05/2024
	* Publicación del Documento		* 30/07/2024
Planificación y control operacional	Seguimiento y control al proceso y procedimientos de Gestión de TI.	Bitácoras de seguimiento y control de acuerdo a los procedimientos.	*18/12/2024
	Elaboración del procedimiento de carnetización.		* 30/04/2024

Gestión del riesgo	Diagnóstico del tratamiento de riesgos de seguridad y privacidad	Informe de seguimiento del plan de tratamiento de riesgos	18/12/2024