PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

DIRECTIVOS

MIGUEL ÁNGEL CANCHALA DELGADO
RECTOR (E)

CARLOS FERNANDO CUELLAR MARTÍNEZ
Vicerrector administrativo

NILSA ANDREA SILVA CASTILLO
Vicerrectora Académica

JULIÁN DARIO GUZMÁN RAMÍREZ
Contratista Gestión Documental y Archivística

Mocoa, Putumayo
Enero de 2021

ÍNDICE.

1. INTRODUCCIÓN

En cumplimiento del artículo 2.2.9.1.3.2. Numeral 2, del Decreto Nacional 1078 de mayo de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, estableciendo metas por cumplir periódicamente y en vista de lo ordenado, el Instituto Tecnológico del Putumayo (ITP) presenta el Plan de Seguridad y Privacidad de la Información para la vigencia 2021.

El Plan de Seguridad y Privacidad de la Información es un instrumento de planeación para la ejecución de actividades y gestiones tendientes a proteger el activo de la información (los servidores públicos, la información, los procesos, las tecnologías de información incluido el hardware y el software) generada en la institución derivada de sus funciones oficiales para un óptimo tratamiento de los riesgos previniendo y evitando el extravió y/o pérdida, vulneraciones y otros que afecten el desarrollo normal de la administración del claustro académico, tanto de información externa como internas garantizando la continuidad de los servicios de la Institución.

Con el fortalecimiento en el procedimiento de la seguridad de la información la Institución busca establecer una cultura por parte de los servidores públicos, concientización y uso de buenas prácticas, permitiendo apoyar los procesos del área TIC. El Instituto Tecnológico del Putumayo como centro educativo de educación superior y cumplidor de la normatividad nacional, identifica y planea las actividades requeridas tendientes a la integridad, confidencialidad y disponibilidad de toda la información oficial que genera producto de su misionalidad y administración; acciones que se plasman en el presente documento público garantizando la transparencia y legalidad en todos sus actos.

2. OBJETIVO

Planear y fortalecer la Seguridad y Privacidad de toda la información del Instituto Tecnológico del Putumayo – ITP en materia de seguridad y privacidad de la información en todo tipo de soporte y por medio de actividades planeadas a corto, mediano y largo plazo, intervenirlas con el fin de subsanarlas para dar cumplimiento a la normatividad colombiana.

3. ALCANCE.

Inicia con el análisis del estado de la seguridad y privacidad de la información, continúa con la planeación y la formulación de proyectos y actividades, posteriormente prosigue la implementación de lo proyectado fase anterior; y finaliza con la evaluación y mejora continua con el objetivo de proteger y garantizar la integridad, confidencialidad y disponibilidad de la información del Instituto Tecnológico del Putumayo – ITP.

4. DEFINICIONES Y SIGLAS.

5.1DEFINICIONES.

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados.
- **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.
- **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
- **Administración de riesgos:** Conjunto de etapas secuenciales que se deben desarrollar para un adecuado tratamiento de los riesgos.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo aceptable.
- **Auditoria:** 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.
- **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.
- **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- **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.

- **Confidencialidad:** Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado.
- **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 aceptado. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. Declaración de aplicabilidad: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo particular.
- **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. Derechos de Autor: es un conjunto.
- **Dato personal:** 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. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **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 que la información sea accesible y utilizable por solicitud de los autorizados.
- **Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
- **Evento de seguridad de la información**: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Gestión de incidentes de seguridad de la Información:** Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización en relación con el 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.

- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos.
- **Mejora Continua:** El seguimiento, revisión y mejora continua del desempeño general del Sistema de Gestión para Registro, alimentan la revisión y mejora del sistema general de la organización.
- **Oficial de datos personales:** Funcionario encargado de coordinar, conocer y verificar que la implementación del Sistema Integral de Gestión de Datos Personales se ejecute de acuerdo con el marco legal vigente.
- **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.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o críticas del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **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.
- **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.
- **Política:** Es el marco referencial o lineamiento general emitido por la Alta Dirección, que orienta para las actuaciones, conductas o funciones de los colaboradores y dependencias.
- **Preservación a Largo Plazo:** Conjunto de acciones y estándares aplicados a los documentos durante su gestión para garantizar su preservación en el tiempo, independientemente de su medio y forma de registro o almacenamiento.
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación.
- **Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.
- **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.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Seguridad y privacidad de la información:** Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.
- **Sistema de Gestión de Seguridad de la Información SGSI:** 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.
- **Sistema Integral de Gestión de Datos Personales:** programa corporativo basado en controles, que responde al tamaño y estructura de la organización, destinado al cumplimiento, implementación y consolidación del régimen de protección de datos.
- **Tratamiento del riesgo:** Proceso de selección e implementación de acciones de mejorar que permita gestionar el riesgo.
- **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.
- **Valoración del riesgo:** Proceso de análisis y evaluación del riesgo.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5.2 SIGLAS.

- **ITP.** Instituto Tecnológico del Putumayo
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **PSPI:** Plan de Seguridad y Privacidad de la Información
- **SGSI:** Sistema de Gestión de Seguridad de la Información

5. DOCUMENTOS DE REFERENCIA.

- Constitución Política de Colombia
- Ley 527 de 1999 Por la cual se define y reglamenta el acceso y uso de mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000 Por medio de la cual se dicta la Ley General de Archivos.
- Ley 1266 de 2008 Por la cual se dictan 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.

- Ley 1581 de 2012 Por la cual se dictan disposiciones para la protección de datos.
- 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.
- Decreto 2693 de 2012 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia.
- Decreto 1377 de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 103 de 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1499 del 11 de septiembre de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1008 del 14 de junio 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.
- Acuerdo 056 de 2000 Por el cual se desarrolla el artículo 45 “Requisitos para Consulta” del capítulo V, “Acceso a documentos de archivo”, del reglamento General de Archivos.
- Acuerdo 060 de 2001 Por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas.
- Acuerdo 038 de 2002 Por el cual se desarrolla el artículo 15 de la Ley General de Archivos. Ley 594 de 2000.
- Acuerdo 042 de 2002 Por el cual se establecen los criterios para la organización de los archivos de gestión en las entidades públicas y privadas que cumplen funciones públicas, se regula el Inventario Único Documental y se desarrollan los artículos 21, 22, 23 y 26 de la Ley General de Archivos. Ley 594 de 2000.
- Acuerdo 006 de 2011 Por el cual se reglamenta la organización y manejo de expedientes pensionales.
- Acuerdo 003 de 2015 Por el cual se establecen los lineamientos generales para las Entidades del Estado en cuanto a la gestión electrónica de documentos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.
- Circular 002 de 1997 Parámetros a tener en cuenta para la implementación de nuevas tecnologías en los archivos públicos.
- Circular 002 de 2012 Adquisición de herramientas tecnológicas de Gestión Documental.
- Circular 005 de 2012 Recomendaciones para llevar a cabo procesos de digitalización y comunicaciones oficiales electrónicas en el marco de la iniciativa cero papel.

- Circular 001 de 2015 Alcance de la expresión "*cualquier medio técnico que garantice su reproducción exacta".*
- Norma ISO 27001:2013
- Resolución 1581 de 2012 y Decreto Reglamentario 1377 de 2013 – Protección de Datos Personales.

6. CONDICIONES GENERALES.

Aprobación del Comité Institucional de Gestión y Desempeño y destinación de recursos para el cumplimiento del Plan de Seguridad y Privacidad de la Información.

7. DESARROLLO DEL CONTENIDO.

Plan de Seguridad y Privacidad de la información

Modelo de Operación por Gestiones de Seguridad y Privacidad de la Información, seguridad digital y continuidad de la Operación.

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital contempla el ciclo de operación el cual consta de cinco (5) fases.

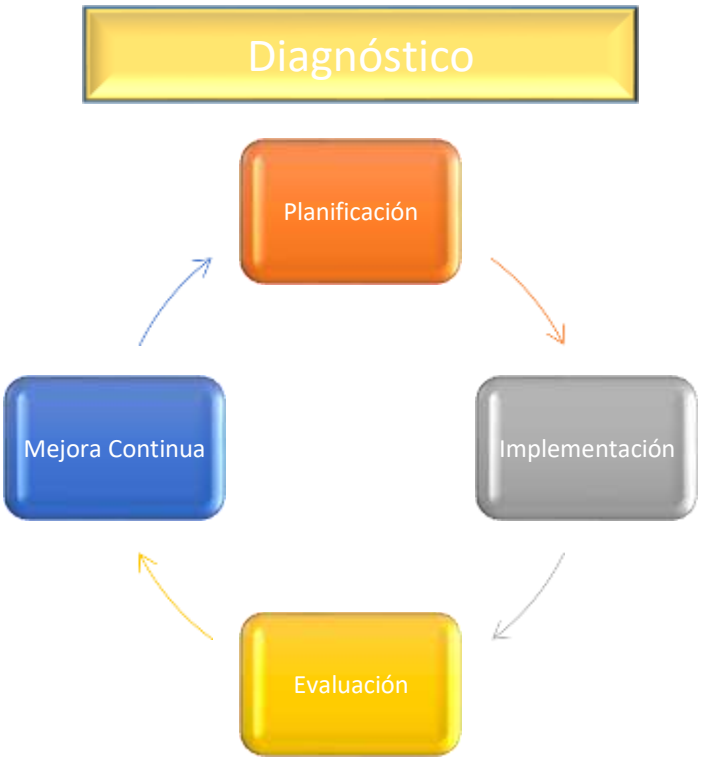

Figura1.Ciclo de operación Modelo de Seguridad y Privacidad de la Información

Tipos de Información

Lo contemplado en el presente Plan, se aplicará a cualquier tipo de información producida y/o recibida por el Instituto Tecnológico del Putumayo - ITP, sus dependencias, funcionarios y contratistas, y en general por cualquier persona que desarrolle actividades inherentes a la función de la institución ó que hayan sido delegados por ésta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en:

A. Documentos de Archivo (físicos y electrónicos).
B. Archivos institucionales (físicos y electrónicos).
C. Sistemas de Información Corporativos.
D. Sistemas de Trabajo Colaborativo. e. Sistemas de Administración de Documentos.
E. Sistemas de Mensajería Electrónica.
F. Portales, Intranet y Extranet.
G. Sistemas de Bases de Datos.
H. Discos duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.
I. Cintas y medios de soporte (back up o contingencia).
J. Uso de tecnologías en la nube.

Características de la Información

a. **Contenido estable.** El contenido del documento no cambia en el tiempo: los cambios deben estar autorizados conforme a reglas establecidas, limitadas y controladas por la institución, o el administrador del sistema, de forma que al ser consultado cualquier documento, una misma pregunta, solicitud o interacción genere siempre el mismo resultado.

b. **Forma documental fija.** Se define como la cualidad del documento de archivo que asegura que su contenido permanece completo y sin alteraciones, a lo largo del tiempo, manteniendo la forma original que tuvo durante su creación.

c. **Vinculo archivístico.** Los documentos de archivo están vinculados entre sí, por razones de la procedencia, proceso, trámite o función y por lo tanto este vínculo debe mantenerse a lo largo del tiempo, a través de metadatos que reflejen el contenido, el contexto y la estructura tanto del documento como de la agrupación documental a la que pertenece.

d. **Equivalente Funcional.** Cuando se requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

e. Conservación. Podrán estar basadas en procesos como la migración, la emulación o el refreshing, o cualquier otro proceso de reconocida capacidad técnica que se genere en el futuro.

Requisitos

Es responsabilidad de la institución cumplir con los elementos esenciales tales como: autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad y conservación, que garanticen que los documentos electrónicos mantienen su valor de evidencia a lo largo del ciclo de vida, incluyendo los expedientes mixtos (híbridos), digitales y electrónicos.

Requisitos para la presunción de autenticidad de los documentos de archivo

a. Se debe expresar desde el momento de su creación los atributos del documento de archivo, tales como el trámite o asunto al que corresponde, las nombres de quienes intervinieron en las diferentes acciones que se llevaron a cabo con el documento, la fecha de creación, la fecha de transmisión, nivel de acceso, los privilegios de acceso, mantenimiento, modificación, transferencia y disposición.
b. Definición de los procedimientos de protección para evitar la pérdida o corrupción de los documentos de archivo, los medios de almacenamiento y la tecnología.
c. Desde el contexto jurídico de acuerdo con lo señalado en el artículo 10° de la Ley 527 de 1999, según el cual en toda actuación administrativa o judicial no se negará eficacia probatoria, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos.
d. Desde el contexto administrativo y documental según las reglas a partir de las cuales el documento de archivo es creado.
e. Formas documentales, autenticación del documento de archivo y su identificación de autoridad.
f. Otra información de ayuda a la verificación de autenticidad a través de metadatos.
g. Establecer procedimientos idóneos para asegurar la cadena de preservación de los documentos electrónicos de archivo a lo largo del ciclo de vida, y en el transcurso del tiempo.

Requisitos para la integridad de los documentos de archivo

Los documentos deben permanecer completos y protegidos de manipulaciones o cualquier posibilidad de cambio (de versión o cambio de un formato); así mismo se debe evitar su alteración o eliminación por personas no autorizadas. En caso de requerirse un cambio a la estructura del documento electrónico, por razones plenamente justificadas y por personal debidamente autorizado, se debe dejar evidencia de dichos cambios en el sistema de gestión documental y en el documento, a través de meta datos.

En el caso que se requiera para garantizar la autenticidad, integridad y confidencialidad de la información, se podrá utilizar firmas electrónicas o digitales de acuerdo con lo señalado en las normas vigentes.

Requisitos para la inalterabilidad de los documentos de archivo

Se debe garantizar que un documento generado por primera vez en su forma definitiva no sea modificado a lo largo de todo su ciclo de vida, desde su producción hasta su conservación temporal o definitiva, condición que puede satisfacerse mediante la aplicación de sistemas de protección de la información, salvo las modificaciones realizadas a la estructura del documento con fines de preservación a largo plazo.

La modificación con fines de preservación a largo plazo no se considerará una alteración del documento electrónico de archivo, siempre que se haga de acuerdo con las normas establecidas por el Archivo General de la Nación Jorge Palacios Preciado y las normas procesales.

Requisitos para la fiabilidad de los documentos de archivo

Garantizan que el contenido de los documentos de archivo es una representación completa, fiel y precisa de las operaciones, las actividades o los hechos que testimonia y por lo tanto, su carácter evidencial asegura que se puede recurrir a estos en el curso de posteriores operaciones o actividades.

Requisitos para la disponibilidad de los documentos de archivo

Los documentos electrónicos y la información en ellos contenida, debe estar disponible en cualquier momento, mientras la entidad está obligada a conservarla, de acuerdo con lo establecido en las Tablas de Retención Documental (TRD).

Se deben establecer mecanismos técnicos que aseguren que la información se pueda consultar y estar disponible en el futuro, independientemente del sistema que la produjo, su estructura o medio de registro original.

Requisitos para la preservación y conservación de los documentos de archivo

a. El documento de archivo debe estar relacionado con las actividades que desarrolla la organización.
b. Se pueden conservar los documentos de archivo simultáneamente en formato análogo y digital de acuerdo a criterios jurídicos, las necesidades de la organización y el valor que las normas procesales, le otorguen a cada formato.
c. El proceso de conservar documentos de archivo se extiende a lo largo de todo el ciclo de vida de los documentos.
d. Resguardar y mantener la accesibilidad de copias auténticas de documentos de archivo digitales.
e. Asegurar que los componentes de los documentos de archivo existirán durante todo el tiempo necesario para que las estrategias de preservación entren en aplicación.

f. las conservaciones de los documentos de archivo deben considerar y atender los principios de preservación en el tiempo, longevidad de los medios de almacenamiento, valoración, vulnerabilidad y disponibilidad, sea que se encuentre en propiedad de los creadores o de las dependencias responsables del archivo de la misma.

g. Teniendo en cuenta que el documento electrónico no es el mismo que era ni antes de ser almacenado ni después de su recuperación, se debe asegurar que cualquier acción que afecte al modo en que se presentan los documentos proteja su integridad, a través del respeto por la cadena de conservación.

h. Proteger la información y los datos personales de conformidad con lo señalado en la ley 1273 de 2009 y ley 1581 de 2012.

Política para el Tratamiento de Riesgos de Seguridad Y Privacidad de la Información

El Instituto Tecnológico del Putumayo adelantará las acciones pertinentes para la implementación y mantenimiento del proceso para el tratamiento de riesgos de seguridad y privacidad de la información, y para ello todos los servidores y contratistas de la institución se comprometen a:

1. Conocer y cumplir las normas internas y externas relacionadas con el tratamiento de riesgos de seguridad y privacidad de la información.
2. Fortalecer la cultura de gestión de riesgos de seguridad y privacidad de la información para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
3. Someter los procesos y procedimientos permanentemente al análisis de riesgos de seguridad y privacidad de la información con base en la aplicación de las metodologías adoptadas para tal efecto.
4. Mantener un control permanente sobre los cambios en la calificación de los riesgos de seguridad y privacidad de la información para realizar oportunamente los ajustes pertinentes.
5. Reportar los eventos de riesgo de seguridad y privacidad de la información que se materialicen, utilizando los procedimientos e instrumentos establecidos para tal efecto.
6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos de seguridad y privacidad de la información que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la institución para así aumentar nuestra eficacia y efectividad.

Implementación

Gestión	Actividades	Tareas	Responsable	Fecha Programación Tareas	
				Fecha inicio	Fecha Final
Activos de la información	Definir lineamientos para el levantamiento de activos de información de las dependencias	Elaboración metodología e instrumento de levantamiento de activos de información	Gestión Documental y Archivística	Febrero 2021	Marzo 2021
	Levantamiento de activos de información	Identificar los activos de información por proceso y/o dependencia	Gestión Documental y Archivística	Febrero 2021	Mayo 2021
		Realizar informe de las novedades encontradas	Gestión Documental y Archivística	Febrero 2021	Mayo 2021
	Publicación y registro de Activos de información	Publicar los instrumentos de activos de información consolidados	Gestión Documental y Archivística – Gestión TIC	Junio 2021	Junio 2021
	Nombramiento y reporte datos personales	Nombrar mediante acto administrativo un oficial de datos personales y/o de seguridad de la información y realizar Reporte al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos	Gestión TIC y oficial de datos personales	Febrero 2021	Mayo 2021
Gestión de Riesgos	Actualización de lineamientos de riesgos	Revisar política y metodología, declaración de aplicabilidad de gestión de riesgos	Gestión TIC	Febrero 2021	Abril 2021
	Socialización	Socialización Plan Modelo de Seguridad y privacidad de la Información y Plan de	Gestión Documental y Archivística –	Abril 2021	Abril 2021

		Continuidad de la operación	Gestión TIC-Talento Humano		
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Gestión Documental y Archivística – Gestión TIC	Febrero 2021	Mayo 2021
		Convocar líderes de procesos a reunión de análisis de riesgos y realizar el acta	Gestión Documental y Archivística – Gestión TIC	Mayo 2021	Mayo 2021
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Líderes de procesos	Mayo 2021	Mayo 2021
	Publicación	Publicación de los riesgos identificados	Líderes de procesos – Gestión TIC	Mayo 2021	Mayo 2021
	Seguimiento Fase de Tratamiento	Seguimiento avance planes de tratamiento de riesgos identificados y verificación de evidencias	Control Interno - Planeación	Mayo 2021	Diciembre 2021
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Control Interno - Planeación	Mayo 2021	Diciembre 2021
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Control Interno - Planeación	Mayo 2021	Diciembre 2021
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	Gestión Documental y Archivística – Gestión TIC	Marzo 2021	Junio 2021
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Gestión Documental y Archivística – Gestión TIC	Junio 2021	Diciembre 2021

Gestión de Incidentes de Seguridad de la Información	Elaboración de procedimiento de gestión de incidentes de seguridad	Elaboración y seguimiento del procedimiento de gestión de incidentes basados en la ISO 27035	Gestión Documental y Archivística – Gestión TIC – Oficina de Calidad - Planeación	Junio 2021	Junio 2021
	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Publicar y socializar el procedimiento de gestión de incidentes de Seguridad de la Información	Gestión Documental y Archivística – Gestión TIC	Julio 2021	Julio 2021
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Gestión Documental y Archivística – Gestión TIC	Julio 2021	Diciembre 2021
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades	Gestión Documental y Archivística – Gestión TIC	Julio 2021	Diciembre 2021
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar, analizar, ejecutar y publicar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional	Gestión Documental y Archivística – Gestión TIC – Oficina de Calidad – Talento Humano	Julio 2021	Diciembre 2021
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación y revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Gestión Documental y Archivística – Gestión TIC – Oficina Jurídica	Abril 2021	Abril 2021
Plan de Continuidad del Negocio	Elaborar documentación del Análisis de Impacto de la Operación	Elaborar y publicar documento de análisis de impacto del negocio	Gestión Documental y Archivística – Gestión TIC – Oficina de Calidad – Planeación	Agosto 2021	Octubre 2021

	Elaborar documentación de Valoración de Riesgos de Interrupción	Actualización y publicación del documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación	Gestión Documental y Archivística – Gestión TIC – Oficina de Calidad – Planeación	Agosto 2022	Noviembre 2021
	Elaborar documentación de Estrategias de Continuidad	Publicación Estrategias de Continuidad de la Operación	Gestión Documental y Archivística – Gestión TIC – Oficina de Calidad – Planeación	Octubre 2021	Noviembre 2021
Acciones correctivas y Notas de mejoras SGSI	Reporte y observaciones del estado de las Acciones Correctivas y Oportunidades de Mejora	Generar reporte de las acciones correctivas y las oportunidades de mejora	Planeación	Junio 2021	Junio 2021
		Hacer el seguimiento a las observaciones realizadas	Control Interno – Planeación	Junio 2021	Diciembre 2021
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la información	Oficial de seguridad de la información - Gestión TIC - Gestión Documental	Febrero 2021	Abril 2021
Gobierno Digital	Gobierno Digital	Elaborar el Plan de Seguridad y Privacidad de la Información.	Gestión Documental	Enero 2021	Enero 2021
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Gestión Documental – Gestión TIC	Febrero 2021	Abril 2021
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Gestión Documental – Gestión TIC	Abril 2021	Noviembre 2021
Auditorías Internas y Externas	Participación en las auditorías internas y	Programar auditorias internas y externas de	Control Interno – Planeación – Gestión TIC –	Marzo 2021 2021	Marzo 2021

	externas de la norma ISO 27001:2013	la norma ISO 27001 : 2013	Gestión Documental		
		Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas	Todos los procesos	Fecha no específica	Diciembre 2021
Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013	Elaborar y aplicar la herramienta para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Gestión TIC – Gestión Documental – Planeación	Fecha no específica	Diciembre 2021
Indicadores	Provisión de información a los indicadores de medición del SGSI	Formular, Implementar, actualizar y reportar los indicadores del SGSI	Gestión TIC – Gestión Documental – Planeación	Febrero 2021	Noviembre 2021
Vulnerabilidades	Contratar Análisis de Vulnerabilidades y Pentest	Procesos de contratación para realizar el pentest y análisis de vulnerabilidades	Vicerrector Administrativo – Gestión TIC – Gestión Documental – Oficina Jurídica	Fecha no específica	Diciembre 2021
	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pentest	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Contratista – Vicerrectoría Administrativa- Gestión TIC – Gestión Documental – Oficina Jurídica	Fecha no específica	Diciembre 2021
	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance y la metodología establecida	Contratista	Fecha no específica	Diciembre 2021
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis	Gestión TIC – Gestión Documental	Fecha no específica	Diciembre 2021

		de vulnerabilidades y pentest			
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC	Oficial de Datos Personales y/o de seguridad de la Información	Marzo 2021	Marzo 2021
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial de Datos Personales y/o de seguridad de la Información	Abril 2021	Abril 2021
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oficial de Datos Personales y/o de seguridad de la Información	Mayo 2021	Agosto 2021