PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2024

MIGUEL ÁNGEL CANCHALA DELGADO
RECTOR

JHON ÁNDRES CERÓN
Vicerrector administrativo

Elaborado por:
JULIÁN DARIO GUZMÁN RAMÍREZ
Contratista Gestión Documental y Archivística

Mocoa, Putumayo
Diciembre de 2024

Contenido

1. INTRODUCCIÓN

Actualmente las infraestructuras informáticas se encuentran expuestas múltiples variedades de amenazas que sin un tratamiento adecuado pueden llegar a penetrar los sistemas de seguridad y afectar del normal desarrollo de las funciones de las organizaciones. Por tal motivo, se hace indispensable definir estrategias que tiendan a identificar los riesgos que se puedan materializarse e interrumpir actividades críticas en las instituciones.

La seguridad se obtiene a partir de la caracterización de los sistemas de información dentro de cada proceso, planteando estrategias y objetivos cuando se identifique un riego que amenace a la institución evitando su materialización mediante una metodología que no permita que el perjuicio se extienda por toda la infraestructura tecnológica causando daños irreparables.

Con el fin de prevenir las intrusiones no autorizadas y dar continuidad a los servicios informáticos, la institución elabora el presente documento como ruta para identificar los posibles riesgos y su valoración minimizando la afectación y restaurando los servicios en el menor tiempo posible. La información del Instituto Tecnológico del Putumayo debe contar con los atributos de integridad, confidencialidad, autenticidad, disponiblidad y no repudio con el fin de que sirva como medio probatorio administrativo y educativo ante los usuarios externos e internos.

2. OBJETIVO

Identificar los riesgos de seguridad y privacidad cuyo objetivo es prevenir su materialización creando un sistema eficaz que permita su restablecimiento y servicios informáticos posterior a cualquier incidente de seguridad que alteren el funcionamiento normal de las actividades administrativas y misionales institucionales.

3. ALCANCE

Inicia con la identificación de los aspectos críticos, su impacto y medición para la priorización de los riesgos potenciales a los que se encuentran expuestos los sistemas de información, su gestión asociados a la infraestructura tecnológica de la institución, servicios, comunicaciones, equipos, software y demás componentes que apoyan el desarrollo del Modelo Integrado de Planeación y Gestión y finaliza con la formulación de actividades y proyectos que los solucionen de manera correctiva o preventiva.

4. DEFINICIONES Y SIGLAS

Definiciones

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Apetito de Riesgo: : Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Capacidad de Riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta a los objetivos. Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos e indirectos sobre los objetivos. Las consecuencias se pueden expresar de manera cualitativa o cuantitativa. Cualquier consecuencia puede incrementarse por efectos en cascada y efectos acumulativos.

Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Contingencia: el algo probable que ocurra en un sistema de información o en un servicio tecnológico, aunque no se tiene certeza al respecto.

Control: Medida que mantiene y/o modifica un riesgo. Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo. Los controles no siempre pueden producir el efecto de modificación previsto o asumido.

Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Es asegurar que la infraestructura, los procesos, las herramientas y las funciones de TI estén adecuados para cumplir con los objetivos del negocio y los niveles de servicio propuestos.

Propiedad de ser accesible y utilizable a demanda por una entidad.

Evento: Es un suceso detectable e importante que ocurre en la infraestructura tecnológica y que puede afectar la prestación del servicio en la organización. Ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias. Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre. Un evento puede ser una fuente de riesgo.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Frecuencia del evento: Puede ser (nunca, aleatoria, periódico y continuo)

Fuente de riesgo: Elemento que, por si solo o en combinación con otros, tiene el potencial de generar riesgo.

Impacto: Es la afectación a nivel organizacional después de ocurrido un evento. Puede ser leve, moderado, grave y muy severo.

Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Nivel de Riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Plan de continuidad: Plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo determinado después de ser detenidas sin autorización o por eventos no controlados.

Parte interesada: Persona u organización que pueda afectar, verse afectada o percibirse como afectada por una decisión o actividad.

Probabilidad: Posibilidad de que algo suceda. Esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos como una probabilidad matemática o una frecuencia en un período de tiempo determinado).

posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Punto de Recuperación Objetivo (RPO) Recovery Point Objetive): Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles. Con

frecuencia, el riesgo se expresa en términos de *fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.*

Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos

Riesgo de Seguridad de la Información: 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. (ISO/IEC 27000).

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Seguridad de la Información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Sistemas Críticos: Son sistemas de información en donde un fallo puede ocasionar pérdidas económicas significativas los cuales soportan los procesos misionales de la entidad.

Tiempo del Trabajo de Recuperación (WRT) Work Recovery Time: Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo.

Tiempo de Recuperación Objetivo (RTO) Recovery Time Objetive: Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

Tiempo Máximo de Inactividad Tolerable (MTD) Maximun Tolerable Downtime: Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la organización empiece a tener pérdidas y debido a esto colapse.

Tolerancia de Riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

Troncal SIP: Canal de comunicaciones telefónicas que se establece entre la entidad y el proveedor a través del canal de fibra que también provee internet.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Siglas

ITP	Instituto Tecnológico del Putumayo
MIPG	Modelo Integrado de Planeación y Gestión

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 599 de 2000** Por el cual se expide el Código Penal.
- **Ley 951 de 2005** Por la cual se crea el acta informe de gestión.
- **Ley 962 de 2005** Por el cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **Ley 1409 de 2010** Por la cual se reglamenta el Ejercicio Profesional de la Archivística, se dicta el Código de Ética y otras disposiciones.
- **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.
- **Ley 1952 de 2019** Por medio del cual se expide el Código General Disciplinario se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario.
- **Decreto 410 de 1971** Por el cual se expide el Código del Comercio.
- **Decreto 019 de 2012** por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **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 1515 de 2013** Por el cual se reglamenta la Ley 80 de 1989 en lo concerniente a las transferencias secundarias y de documentos de valor histórico al Archivo General de la Nacional, a los Archivos Territoriales, se derogan los Decretos 1382 de 1995 y 998 de 1997 y se dictan otras disposiciones.
- **Decreto 1080 de mayo de 2015** Por medio del cual se expide el Decreto Reglamentario único del sector cultura.
- **Decreto 103 de 2015** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1008 de 2018 art. 2.2.9.1.1.3** 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.

- **Decreto 2106 de 2019** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Acuerdo 011 de 1996** Por el cual se establecen criterios de conservación y organización de documentos.
- **Acuerdo 047 de 2000** Por el cual se desarrolla el capítulo V "Acceso a documentos de archivo" del Archivo General de la Nación, del Reglamento General de Archivos sobre "Restricciones por razones de conservación".
- **Acuerdo 049 de 2000** Por el cual se desarrolla el artículo del Capítulo 7 "Conservación de documentos" del Reglamento General de Archivos sobre "Condiciones de edificios y locales destinados a archivos".
- **Acuerdo 050 de 2000** Por el cual se desarrolla el artículo 64 del Título VII "Conservación de Documento", del Reglamento General de Archivos sobre "Prevención de deterioro de los documentos de archivo y situaciones de riesgo."
- **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 016 de 2002** Por el cual se adopta la política archivística y se dictan otras disposiciones para el manejo de los archivos públicos de las Cámaras de Comercio.
- **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 002 de 2004** Por el cual se establecen los lineamientos básicos para la organización de Fondos Acumulados.
- **Acuerdo 027 de 2006** por el cual se modifica el Acuerdo 007 de 1994.
- **Acuerdo 006 de 2011** Por el cual se reglamenta la organización y manejo de expedientes pensionales.
- **Acuerdo 003 de 2013** por el cual se reglamenta parcialmente el Decreto 2578 de 2012, se adopta y reglamenta el Comité Evaluador de Documentos del Archivo General de la Nación y se dictan otras disposiciones.
- **Acuerdo 004 de 2013** Por el cual se reglamentan parcialmente los Decretos 2578 y 2609 de 2012 y se modifica el procedimiento para la elaboración, presentación, evaluación, aprobación e implementación de las Tablas de Retención Documental y las Tablas de Valoración Documental.
- **Acuerdo 005 de 2013** Por medio del cual se establecen los criterios básicos para la clasificación, ordenación y descripción de los archivos en las entidades públicas y privadas que cumplen funciones públicas y se dictan otras disposiciones.

- **Acuerdo 002 de 2014** por medio del cual se establecen los criterios básicos para la creación, conformación, control y consulta de los expedientes de archivo y se dictan otras disposiciones.
- **Acuerdo 006 de 2014** Por medio del cual se desarrollan los artículos 46, 47 y 48 del Título XI Conservación de Documentos" de la Ley 594 de 2000.
- **Acuerdo 007 de 2014** por medio del cual se establecen los lineamientos para la reconstrucción de expedientes y se dictan otras disposiciones.
- **Acuerdo 008 de 2014** por medio del cual se establecen las especificaciones técnicas y los requisitos para la prestación de los servicios de depósito, custodia, organización, reprografía y conservación de documentos de archivo y demás procesos de la función archivística en desarrollo de los artículos 13 y 14 y sus parágrafos 1 y 3 de la Ley 594 de 2000.
- **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.
- **Acuerdo 004 de 2015** por el cual se reglamenta la administración integral, control conservación, posesión, custodia y aseguramiento de documentos públicos relativos a los Derechos Humanos y el Derecho Internacional Humanitario que se conservan en las Entidades del Estado.
- **Circular 002 de 1997** Parámetros a tener en cuenta para la implementación de nuevas tecnologías en los archivos públicos.
- **Circular 13 de 1999** Producción documental: Uso de tintas de escritura.
- **Circular 007 de 2002** Organización y conservación de los documentos de archivo de las entidades de la rama ejecutiva del orden nacional.
- **Circular 004 de 2003** Organización de Historias Laborales.
- **Circular 012 de 2004** Orientación para el cumplimiento de la circular nro. 004 de 2003. (organización de historias laborales).
- **Circular 001 de 2011** protección de archivos por ola invernal.
- **Circular 004 de 2011** Directrices o lineamientos al manejo y administración de los archivos señalados en la Ley 1444 de 2011.
- **Circular 005 de 2011** prohibición de enviar los originales de documentos de archivo a otro tipo de unidades de información.
- **Circular 002 de 2012** Adquisición de herramientas tecnológicas de Gestión Documental.
- **Circular 003 de 2012** Responsabilidad del AGN y del SNA respecto de los archivos de DDHH y memoria histórica en la implementación de la ley 1448 de 2011, Ley de Víctimas.
- **Circular 004 de 2012** Censo de archivos e inventario documental relacionados con la atención a víctimas del conflicto armado en Colombia.
- **Circular 005 de 2012** Recomendaciones para llevar a cabo procesos de digitalización y comunicaciones oficiales electrónicas en el marco de la iniciativa cero papel.

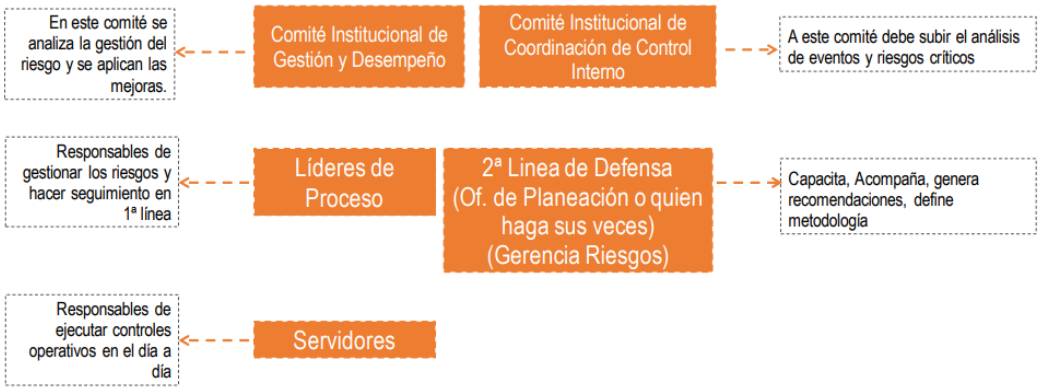
- **Circular 001 de 2014** Cumplimiento de la Ley 594 de 2000, el Decreto 2578 de 2012, el Decreto 2609 de 2012 y el Decreto 1515 de 2013.
- **Circular 001 de 2015** Alcance de la expresión "*cualquier medio técnico que garantice su reproducción exacta".*
- **Circular 002 de 2015** Entrega de archivos, en cualquier soporte, con ocasión del cambio de administración en las entidades territoriales.
- **CONPES 3854** Política Nacional de Seguridad Digital.
- **ISO 27001: 2013** Sistema de Gestión de Seguridad de la Información.

6. CONDICIONES GENERALES

- Identificar el mapa de procesos y su caracterización, objetivos estratégicos, cadena de valor, Misión y Visión.
- Recopilar e identificar los activos de información, clasificarlos y su nivel de criticidad.
- Elaborar una metodología para la identificación y valoración de los riesgos identificados con sus niveles, manejo, tabla de impactos.
- Definir la periodicidad para el monitoreo y revisión de los riesgos.
-

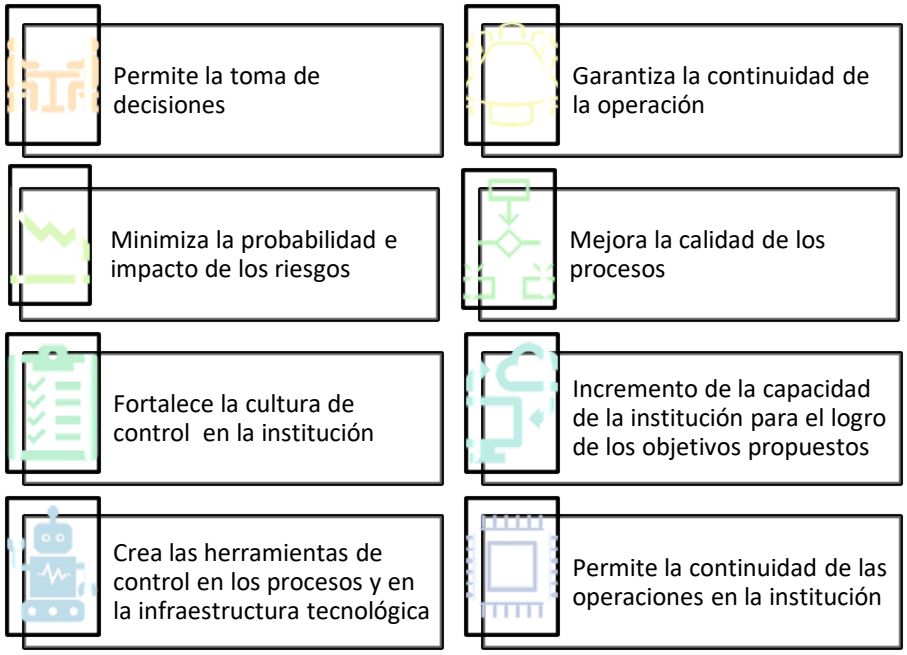
7. DESARROLLO DEL CONTENIDO

Para el cumplimiento del presente plan debe involucrarse la Alta Dirección (Rectoría y Vicerrectorías Académica y Administrativa) liderada en este caso por el área de Tecnologías de la Información o su denominación en la Institución y por Gestión Documental y Archivística quien ha venido acompañando los diferentes planes de seguridad de la información debido a su carácter transversal. El Modelo Integrado de Planeación y Gestión (MIPG) y el Comité Institucional de Coordinación de Control Interno entran a operar para una adecuada gestión del riesgo y se visualiza en la siguiente gráfica:



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

La gestión de riesgos informáticos tiende a prevenir, identificar, evitar, minimizar, controlar y dar continuidad a las operaciones básicas de la institución generando beneficios tales como:



El Modelo Integrado de Planeación y Gestión (MIPG) establece que el Direccionamiento Estratégico y de Planeación emite los lineamientos precisos para el tratamiento, manejo y seguimiento de los riesgos que afectan el logro de los objetivos institucionales; El Plan de Tratamiento de los Riesgos de Seguridad y Privacidad de la Información coadyuva a la planeación del trabajo que se debe adelantar mediante una metodología precisa con actividades operativas de las áreas de tecnología o quien haga sus veces en el ITP, y de gestión documental y archivística como especialistas en seguridad de la información.

El Estado Colombiano plantea la metodología mediante una estructura para la gestión del riesgo la cual se tomará como sugerencia para el desarrollo del presente plan estratégico.

1- Determinación de la capacidad de riesgo
   a. Valor máximo de la escala que resulta de combinar la probabilidad y el impacto
   b. Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la institución, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad de riesgo.

2- Determinación del apetito de riesgo
   a. Valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la institución.
3- Tolerancia de riesgo
   a. Valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la institución. se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo. El límite o valor de la tolerancia de riesgo es definido por la alta dirección (Rectoría, Vicerrectorías Académica y Administrativa) y aprobada por el Comité Institucional de Gestión y Desempeño y no puede ser superior al valor de la capacidad de riesgo. se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

Tomando como base el Plan de Privacidad y Seguridad de la Información del ITP en su punto 2 denominado *Gestión de Riesgos* plantea una serie de actividades que se deben implementar con el fin de identificar y prevenir la materialización de las amenazas que pueden llegar a interrumpir la operación normal de la institución.

	Actividades	Tareas	Responsable	Fecha Programación Tareas		Observaciones
				Fecha inicio	Fecha Final	
	Actualización de lineamientos de riesgos	Elaborar y/o revisar política y metodología, declaración de aplicabilidad de gestión de riesgos	Gestión Documental y Archivística - Sistemas	Enero 2024	Diciembre 2024	Inicia una vez se tengan identificados los activos de información
	Socialización	Socialización Plan Modelo de Seguridad y privacidad de la Información y Plan de Continuidad de la operación	Gestión Documental y Archivística - Sistemas	Septiembre 2024	Septiembre 2024	Actividad que se ejecuta una vez se tenga elaborado el Plan de Continuidad del Negocio Fecha indeterminada
	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 - Sistemas	Agosto 2024	Agosto 2024	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación
		Convocar líderes de procesos a reunión de análisis de riesgos y realizar el acta	Gestión Documental y Archivística - Sistemas	Septiembre 2024	Septiembre 2024	Convocar líderes de procesos a reunión de análisis de riesgos y realizar el acta

Gestión de Riesgos	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Líderes de procesos	Septiembre 2024	Septiembre 2024	Aceptación, aprobación Riesgos identificados y planes de tratamiento
	Publicación	Publicación de los riesgos identificados	Líderes de procesos – Gestión TIC	Septiembre 2024	Septiembre 2024	La publicación se realiza una vez elaborado el informe de los riesgos públicos identificados
	Seguimiento Fase de Tratamiento	Seguimiento avance planes de tratamiento de riesgos identificados y verificación de evidencias	Control Interno - Planeación	Septiembre 2024	Diciembre 2024	Actividad sujeta a la identificación de los riesgos y el plan correspondiente
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Control Interno - Planeación	Septiembre 2024	Diciembre 2024	Actividad sujeta al seguimiento de los riesgos y el plan correspondiente
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Control Interno - Planeación	Septiembre 2024	Diciembre 2024	Actividad sujeta a la evaluación de los riesgos y el plan correspondiente
		Elaboración y/o actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados	Gestión Documental y Archivística - Sistemas	Enero 2025	Abril 2025	Sujeta a la contratación
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Gestión Documental y Archivística - Sistemas	Agosto 2025	Agosto 2025	Sujeta a la contratación

Para el desarrollo del Plan propuesto se seguirán los siguientes pasos.

Fases del desarrollo del Plan


Planear
• Definición de actividades y Responsables
• Identificación de responsables
• Definición de cada actividad
• Objetivos de cada actividad
Hacer
• Análisis de los activos de información
• Identificación de activos
• Clasificación
• Nivel de criticidad
• Riesgos asociados
• Controles
• Se evalúa cada activo, su clasificación, nivel de criticidad y riesgos asociados
Verificar
• Desarrollo de las medidas por tomar para cada activo
• Determinar las medidas por tomar y su efectividad
• Evaluar la actividad de cada responsable
• Validar las actividades
Actuar
•Controles
•Identificación de los controles por activo
•Validación y justificación de cada control
•Actividad de mitigación de riesgos
•Evaluación del riesgo