TRANSMETRO S.A.S

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

Subgerencia Administrativa – Área de Sistemas

Tabla de contenido

1. Introducción

Transmetro en busca de la mejora continua implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma. La institución en su quehacer diario utiliza TIC en cuanto a captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes actores del sistema, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos por lo cual este documento busca establecer un línea de trabajo que permita a la entidad sortear los riesgos que lo rodean y lograr que su información este segura.

2. Objetivos

2.1. Objetivos Generales

Desarrollar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información el cual sea una guía para el control y minimización de los de los riesgos y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la institución.

2.2. Objetivos Específicos

Lograr un diagnóstico real de la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información - Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y Mintic para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información - Optimización de los recursos de la institución en la aplicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

3. Alcance

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

4. Términos y Definiciones

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. (ISO/IEC 27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditoría: 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. (ISO/IEC 27000).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española). 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 asumido. 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: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

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. (ISO/IEC 27000).

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. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados 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. (ISO/IEC 27000).

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. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

5. Marco Legal

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

6. Requisitos Técnicos

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Procesos de Cobit 5, relacionados con la continuidad del negocio y gestión del riego.

7. Descripción del Plan

Para establecer el plan de implementación se generó la siguiente tabla con los procesos definidos en el Mapeo entre las metas relacionadas con TI y los procesos de Cobit 5, ordenados según el puntaje obtenido y con el fin de establecer la prioridad de implementación dentro de las 3 fases contempladas para el caso de estudio.

Figura 1. Priorización de Procesos de Cobit 5 para TM

DSS04	Gestionar la Continuidad	1	5	5	1	1	5	1	19
APO13	Gestionar la Seguridad		5	1	1	5	5		17
DSS03	Gestionar los Problemas		5	5	1		5	1	17
BAI06	Gestionar los Cambios		5	5	1	5			16
APO09	Gestionar los Acuerdos de Servicio	1	1	5	1	1	5	1	15
DSS05	Gestionar los Servicios de Seguridad	1	5	1	1	5	1	1	15
EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	5	1	5		1	1	1	14
EDM03	Asegurar la Optimización del Riesgo	1		1	1	5	1	5	14
APO01	Gestionar el Marco de Gestión de TI	5	1	1		1	1	5	14
APO02	Gestionar la Estrategia	5	1	5	1		1	1	14
APO10	Gestionar los Proveedores		5	5	1	1	1	1	14
APO12	Gestionar el Riesgo		5	1	1	5	1	1	14
BAI02	Gestionar la Definición de Requisitos	5	1	5	1	1	1		14
DSS01	Gestionar las Operaciones		5	5	1	1	1	1	14
DSS02	Gestionar las Peticiones y los Incidentes del Servicio		5	5	1	1	1	1	14
DSS06	Gestionar los Controles de los Procesos del Negocio		5	5	1	1	1	1	14
APO08	Gestionar las Relaciones	5	1	5	1			1	13
EDM02	Asegurar la Entrega de Beneficios	5		5	1		1		12
BAI01	Gestionar los Programas y Proyectos	5	5	1	1				12
BAI04	Gestionar la Disponibilidad y la Capacidad		1	5	1		5		12
BAI05	Gestionar la introducción de Cambios Organizativos	1		5	1		5		12
APO11	Gestionar la Calidad	1	1	5	1	1	1	1	11
EDM04	Asegurar la Optimización de los Recursos	1	1	1	1		1	5	10
APO03	Gestionar la Arquitectura Empresarial	5	1	1	1	1	1		10
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	1		5	1	1	1	1	10
APO04	Gestionar la Innovación	1	1	1	5		1		9
APO05	Gestionar el Portafolio	5	1	1	1		1		9
APO07	Gestionar los Recursos Humanos	5	1	1		1		1	9
BAI03	Gestionar la Identificación y la Construcción de Soluciones	1	1	5	1		1		9
BAI07	Gestionar la Aceptación del Cambio y de la Transición		1	1	5		1	1	9
BAI10	Gestionar la Configuración		1		1	1	5	1	9
EDM05	Asegurar la Transparencia hacia las partes interesadas	1		5			1	1	8
BAI09	Gestionar los Activos	1	1	1	1		1	1	6
BAI08	Gestionar el Conocimiento	1		1	1	1	1		5
MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno			1	1	1	1	1	5
APO06	Gestionar el Presupuesto y los Costes	1	1	1	1				4
MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos			1		1		1	3

Fuente: elaboración propia.

En segundo lugar es necesario identificar el nivel de capacidad de cada proceso de TI, con el propósito de definir la brecha entre el estado actual y el nivel deseado que para nuestro caso de estudio el mínimo aceptable es Nivel 3, y así determinar la mejor forma de implementar todos los procesos, teniendo en cuenta los objetivos estratégicos de la entidad.

Por lo cual, se ha realizado el análisis de capacidades con la guía de autoevaluación de COBIT 5 (COBIT® Self-assessment Guide: Using COBIT® 5, 2013) que propone una metodología de evaluación que "está diseñada para proporcionar a las empresas una metodología repetible, confiable y robusta para evaluar la capacidad de sus procesos de TI" (COBIT® Self-assessment Guide, 2013, pág. 7). La evaluación se efectuó en base a los siguientes niveles de capacidad de los procesos:

Figura 2. Process capability levels.

Figure 2—Process Capability Levels	
Process Level	**Capability**
0 (Incomplete)	The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
1 (Performed)	The implemented process achieves its process purpose.
2 (Managed)	The performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
3 (Established)	The managed process is now implemented using a defined process that is capable of achieving its process outcomes.
4 (Predictable)	The established process now operates within defined limits to achieve its process outcomes.
5 (Optimizing)	The predictable process is continuously improved to meet relevant current and projected business goals.

Fuente: Tomada de Cobit Self assessment.

Además Se utilizó la siguiente escala de calificación definida en COBIT 5 para evaluar cada proceso:

- **N** (No conseguido): Consecución del 0 a 15%, ausencia o poca evidencia de la misma.
- **P** (Parcialmente conseguido): Consecución entre 15% al 50%, se dispone de alguna prueba del logro.
- **L** (Ampliamente conseguido): Consecución entre 50% al 85%, se observan pruebas de un nivel significativo de consecución del atributo definido.
- **F** (Totalmente conseguido): Consecución entre 85% al 100%, es decir un nivel total de logro. (*COBIT® Self-assessment Guide: Using COBIT® 5*, 2013, pág. 11)

En la siguiente figura se muestra el resumen de los resultados obtenidos de la evaluación de capacidades.

Figura 3. Niveles de Capacidad de Transmetro.

EDM01		
EDM01	Nivel de Capacidad	Nivel Objetivo
Nivel 1 - Ejecutado	1	3
EDM03		
EDM03	Nivel de Capacidad	Nivel Objetivo
Nivel 1 - Ejecutado	1	3
APO01		
APO01	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
APO02		
APO02	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
APO08		
APO08	Nivel de Capacidad	Nivel Objetivo
Nivel 1 - Ejecutado	1	3
APO09		
APO09	Nivel de Capacidad	Nivel Objetivo
Nivel 2 - Gestionado	2	4
APO10		
APO10	Nivel de Capacidad	Nivel Objetivo
Nivel 2 - Gestionado	2	4
APO12		
APO12	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
APO13		
APO13	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
BAI01		
BAI01	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
BAI02		
BAI02	Nivel de Capacidad	Nivel Objetivo
Nivel 2 - Gestionado	2	4
BAI06		
BAI06	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
DSS01		
DSS01	Nivel de Capacidad	Nivel Objetivo
Nivel 3 Establecido	3	4
DSS02		
DSS02	Nivel de Capacidad	Nivel Objetivo
Nivel 3 Establecido	3	4
DSS03		
DSS03	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
DSS04		
DSS04	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
DSS05		
DSS05	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	3
DSS06		
DSS06	Nivel de Capacidad	Nivel Objetivo
Nivel 0 - Incompleto	0	1

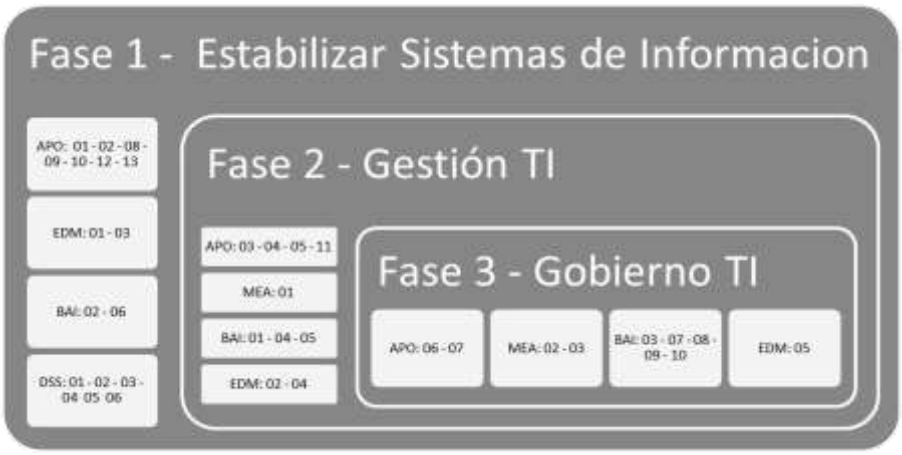
Fuente: elaboración propia.

En base a los resultados obtenidos en el nivel de capacidades actual de cada proceso, en la Figura 3. Niveles de Capacidad de Transmetro, se coloca el nivel de capacidad objetivo que se tiene contemplado para la primera Fase; y una vez alcanzado dicho objetivo se continuará con las siguientes fases hasta alcanzar el nivel de capacidad máximo. Se determinaron los siguientes criterios para establecer los niveles de capacidad objetivo para cada proceso y poder desarrollar las observaciones, recomendaciones y directrices, para cerrar las brechas y alcanzar al nivel deseado, en base al mínimo nivel aceptable para el caso de estudio - Nivel 3:

- Los procesos de TI que se encuentren en un nivel de capacidad 0 (Incompleto) y 1 (Ejecutado), deberán cerrar las brechas para lograr que el proceso sea 3 (Establecido).
- Los procesos de TI que se encuentren en el nivel 2 (Gestionado) y 3 (Establecido), deberán cerrar las brechas para alcanzar un nivel 4 (Predecible).

Debido a que los procesos de TI determinados en el modelo son numerosos, se ha definido que la implementación sea realizada en 3 fases basadas en la prioridad obtenida como resultado de la evaluación de capacidades de cada proceso, en la primera fase se tendrán en cuenta los procesos por encima del promedio de la autoevaluación y en las 2 fases siguientes , se distribuirán los 20 procesos faltantes, teniendo en cuenta su valoración, cabe resaltar que una vez implementados los procesos que se encuentran más alineados con el negocio, estos constituirán una base para desarrollar con mayor facilidad los demás procesos, pero a su vez representa un reto debido a que se encuentran en gran parte en un nivel de capacidad 0. a continuación, se detallan los procesos según la fase correspondiente.

Figura 4. Fases de Implantación



Fuente: elaboración propia.

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas recolectan datos de entrada para esta actividad.

a. Implementar la Gestión de Riegos de TI y de Continuidad del Negocio.

1. Procesos:

Construir, Adquirir e Implementar	Alinear, Planificar y Organizar	Entregar, dar Servicio y Soporte
• **BAI06**	• **APO12**	• **DSS04** • **DSS05** • **DSS06**

2. Descripción:

Para implementar la Gestión de Riesgos de TI, la Alta Gerencia primero deberá definir el Marco de Riesgos de TI. Este marco deberá estar basado en determinados principios generales: la gestión efectiva de riesgos de TI debe estar alineada con los objetivos de la empresa y con un marco de gestión de riesgo empresarial (ej. Enterprise Risk Management). Este marco abarca tres dominios: Gobierno de Riesgos, Evaluación de Riesgos, y Respuesta a Riesgos. En base al Marco definido, la Empresa Transmetro deberá crear y dar mantenimiento a los procesos de gestión de riesgos. Estos procesos deberán documentar un nivel común y acordado de riesgos de TI, estrategias de mitigación y manejo de riesgos residuales. Cualquier impacto potencial sobre las metas de la organización causada por algún evento no planeado, se debe identificar, analizar y evaluar.

Además se deberá desarrollar un plan que permita gestionar la continuidad de negocio, que será la guía para la recuperación de desastres y de contingencias, estableciendo los roles, las tareas y responsabilidades del personal interno y externo de la estructura organizacional; así como los procedimientos para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. Los planes de continuidad deberán estar diseñados para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Probar el plan de continuidad de TI de forma periódica para probar su efectividad del mismo y realizar las correcciones que permitan el mejoramiento continuo del mismo.

3. Actividades principales:

- Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI.
- Alinear la perspectiva con los objetivos de la empresa y con el marco de ERM.
- Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.
- Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio.
- Evaluar y seleccionar las respuestas a riesgos de TI.
- Priorizar y planear actividades de control.
- Aprobar y confirmar fondos para planes de acción de riesgos.
- Mantener y monitorear el plan de acción de riesgos.
- Probar el plan de continuidad de TI de forma periódica.
- Incluir los cambios en la documentación que hace parte de la continuidad de negocio y recuperación frente a desastres.
- Identificar las partes interesadas claves, los roles y responsabilidades para definir y acordar la política de continuidad y su alcance.
- Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI.
- Identificar los requerimientos de recursos y costes para cada opción

técnica estratégica y realizar recomendaciones estratégicas.

- Asegurar que los proveedores y socios externos clave tengan implantados planes de continuidad efectivos
- Obtener la aprobación de los ejecutivos de negocio para las opciones estratégicas seleccionadas.

4. Métricas:

- Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento.
- Porcentaje de medios de respaldo transferidos y almacenados de forma

  segura.
- Porcentaje de interesados internos y externos que han recibido formación.
- Número de ejercicios y pruebas que han conseguido los objetivos de recuperación.
- Porcentaje de mejoras acordadas que han sido reflejadas en el plan
- Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan
- Frecuencia de las pruebas.