TRANSMETRO S.A.S

Plan de Seguridad y Privacidad de la Información

Subgerencia Administrativa – Área de Sistemas

Tabla de contenido

Tabla de contenido 1
1. Introducción 2
2. Objetivos 2
1.1. Objetivo General 2
1.2. Objetivo Especifico 2
3. Alcance 2
4. Términos y Definiciones 2
5. Marco Legal 4
6. Requisitos Técnicos 4
7. Descripción del Plan 4

1. Introducción

Este documento busca lograr la implementación en Transmetro S.A.S de las mejoras prácticas dadas por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información. El Modelo de Seguridad y Privacidad de la Información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

2. Objetivos

1.1. Objetivo General

Generar un documento institucionales guiado en de lineamientos de buenas prácticas en seguridad y Privacidad de la información.

1.2. Objetivo Especifico

- Promover el uso de mejores prácticas de seguridad de la información en la institución.
- Optimizar la gestión de la seguridad de la información al interior de le entidad.
- Aplicar de manera correcta la legislación relacionada con la protección de datos personales.
- Optimizar la labor de acceso a la información pública.

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

El equipo de colaboradores y el Gerente de Transmetro S.A.S se comprometen a garantizar la confidencialidad, seguridad e integralidad de la información de los usuarios y su familia, clientes internos y externos en cuanto a seguridad lógica y física de los activos, fomento de canales de comunicación que garanticen acceso y transparencia de la información pública a través de uso adecuado de las TICS, cumpliendo con las disposiciones generales para la protección de datos, aportando al cumplimiento de la Misión, Visión y objetivos estratégicos de la institución.

a. Asegurar el Entrenamiento y Soporte a usuarios.

1. Procesos:

Evaluar, Orientar y Supervisar	Alinear, Planificar y Organizar	Entregar, dar Servicio y Soporte
• **EDM03**	• **APO08** • **APO09**	• **DSS01** • **DSS02** • **DSS03** • **DSS04** • **DSS05** • **DSS06**

2. Descripción:

Transmetro deberá capacitar a los empleados, en cuanto a lis riesgos del mal uso de las ti, por lo cual deberá divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención, También capacitarlos en el uso e implementación de nuevos softwares e infraestructura de TI. Se deberá implementar un plan de pruebas de los respaldos y backup de los sistemas de información de la entidad.

Para mejorar el soporte prestado a los usuarios, se deberá implementar una de mesa de servicio de manera que se pueda realizar la gestión adecuada a cada caso de acuerdo con los niveles de servicio establecidos y, si es adecuado, brindar soluciones alternas. Cuando se resuelva un incidente, la mesa de servicios deberá registrar la causa raíz, con el fin de mantener un catálogo de gestión de problemas único para registrar e informar sobre problemas identificados. También se deberá emitir reportes y análisis de las tendencias de incidentes y problemas recurrentes para mejorar continuamente el diseño y operación de los controles de procesos de negocio.

3. Actividades principales:

- Identificar y categorizar las necesidades de capacitación de los usuarios.
- Asegurar que se cumple con los estándares de seguridad aplicables

para la recepción, procesamiento, almacenamiento y salida de datos de forma tal que se satisfagan los objetivos empresariales, la política de seguridad de la empresa y los requerimientos regulatorios.

- Programar, realizar y registrar las copias de respaldo de acuerdo con las políticas y procedimientos establecidos.
- Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.
- Definir esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas, para asegurar

  enfoques consistentes en el tratamiento, informando a los usuarios y realizando análisis de tendencias.
- Mantener un catálogo de gestión de problemas único para registrar e informar sobre problemas identificados y para establecer pistas de auditoría

  sobre los procesos de gestión de problemas, incluyendo el estado de cada problema (p. ej., abierto, reabierto, en progreso o cerrado).
- Informar del estado de problemas identificados al centro de servicios de forma que los clientes y la gestión de TI pueden mantenerse informados.
- Identificar procesos de soporte al negocio esenciales y servicios TI relacionados.
- Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.

- Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de

  cambios.
- Mejorar continuamente el diseño y operación de los controles de procesos de negocio.

4. **Métricas:**

- Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio.
- Porcentaje de incidentes resueltos dentro de un periodo acordado/aceptable.
- Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento.
- Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo.
- Frecuencia de las pruebas.
- Número de incidentes relacionados con accesos no autorizados a la información.

El siguiente plan está diseñado para cumplir la fase de determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.