1. OBJETIVOS

- Asegurar la confidencialidad, integridad y disponibilidad de los activos de información de TGI S.A. ESP, mediante la implementación de las directrices, políticas, reglamento, procedimientos, controles y demás lineamientos de seguridad de la información.

- Gestionar los riesgos de seguridad de la información, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

- Crear y mantener una cultura de seguridad de la información, a través de la divulgación y sensibilización de las directrices, políticas, reglamento, lineamientos, y demás normatividad vigente y aplicable en temas de seguridad y privacidad a todas las partes interesadas del MSPI.

- Gestionar de manera precisa, oportuna y efectiva, los incidentes de seguridad de la información siguiendo los procedimientos, controles y lineamientos definidos, con el fin de reducir el impacto en las actividades administrativas y operativas de TGI S.A. ESP.

- Contribuir a la continuidad de los servicios y operaciones de TGI S.A. ESP., definiendo un plan de gestión de recuperación de desastres y continuidad de TI.

- Cumplir con el marco normativo y legal vigente, aplicable a TGI S.A. ESP., en temas de privacidad y seguridad de la información

2. ALCANCE

TGI S.A. ESP., establece e implementa el Modelo de Seguridad de la Información (MSPI), que busca proteger la Confidencialidad, Integridad y Disponibilidad de los activos de información, para su Sede Administrativa ubicada en la Carrera 9 No. 73-44 en Bogotá, y todas las demás sedes a Nivel Nacional, el cual cuenta con el apoyo de la Alta Dirección para garantizar los recursos necesarios para la mejora continua del modelo, y para exigir el cumplimiento de las directrices, políticas y demás lineamientos de seguridad que se definan, los cuales deben ser conocidos, entendidos y aceptados por todas las partes interesadas del Modelo de Seguridad y Privacidad de la Información (MSPI).

3. DEFINICIÓN DE TÉRMINOS

3.1 ACTIVO: Cualquier cosa que tenga valor para un individuo, una organización o un gobierno.
3.2 ACTIVO DE INFORMACIÓN: Conocimiento o datos que tienen valor para el individuo u organización.
3.3 ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.
3.4 CONFIDENCIALIDAD: Propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.
3.5 DISPONIBILIDAD: Propiedad de ser accesible y utilizable a pedido de una entidad autorizada.
3.6 INTEGRIDAD: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.
3.7 NIVEL DE CLASIFICACIÓN: Para cada propiedad de seguridad de la información (Confidencialidad, Integridad, Disponibilidad) se establecieron criterios específicos y lineamientos para el tratamiento adecuado del activo. Los niveles y criterios de cada una se detallan en la Guía de Gestión de Activos.
3.8 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.

COPIA NO CONTROLADA

3.9 PROCEDIMIENTO: Forma especificada de llevar a cabo una actividad o un proceso.

3.10 USUARIO: Son todos los trabajadores, contratistas, judicantes, practicantes, aprendices SENA, entes de control y demás terceros que tengan acceso o uso de los activos de información de TGI S.A. ESP.

3.11 VULNERABILIDAD: Debilidad de un activo o control que puede ser explotado por una o más amenazas.

3.12 CIBERSEGURIDAD: Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

4. DESARROLLO DE ACTIVIDADES

TGI S.A. ESP establece e implementa el Modelo de Seguridad y Privacidad de la Información (MSPI), alineado a su visión, estrategia, valores y al Sistema Integrado de Gestión, para lo cual define las políticas y demás lineamientos de seguridad y privacidad de la información, con el fin de preservar la integridad, disponibilidad y confidencialidad de la información, de acuerdo a lo definido por la compañía dentro del Sistema Integrado de Gestión, que a su vez está alineado al Sistema de Gestión de Calidad, el cual cuenta con la estructura documental para responder a todas las necesidades y requisitos de obligatorio cumplimiento.

De acuerdo con lo anterior, el Modelo de Seguridad y Privacidad Gestión de Seguridad de la Información, el cual está alineado al modelo de seguridad de la información y ciberseguridad de GEB, adopta la estructura documental, y todos los lineamientos del Sistema Integrado de Gestión, lo que permite fortalecer los procesos y optimizar los recursos de TGI S.A. ESP., y a su vez cumple con la normatividad legal, y todos los requisitos incluidos dentro del Sistema de Gestión de Calidad.

En TGI se trabaja para brindar servicio de calidad e innovación, motivando y orientado a la consecución de logros de manera eficiente. A través de la gestión transparente y la búsqueda continua de la excelencia, contribuyendo al desarrollo de la industria y al crecimiento del país.

El MSPI apoya de forma transversal a la consecución de los objetivos estratégicos enmarcados en los pilares del negocio que, a partir del cumplimiento riguroso de los códigos de ética y buen gobierno, enmarcan la estrategia de TGI:

Pilares TGI

4.1 PARTES INTERESADAS

TGI S.A. ESP., crea y provee soluciones integrales de la industria de hidrocarburos (midstream) de baja emisión (gas natural y posiblemente GLP y/o biogás, y otros gases en el futuro: hidrógeno, etc.) a

COPIA NO CONTROLADA

grandes usuarios, productores y desarrolladores de mercados energéticos, conectando fuentes con centros de consumo, a través de relaciones de largo plazo y negocios intensivos en capital.

TGI S.A. ESP., comprometida en prestar servicios de calidad mediante el desarrollo de mejores prácticas, motiva a gestionar nuevos y mejores canales de información y comunicación con los grupos de interés.

La Oficina de Relación con Inversionistas del Grupo Energía Bogotá tiene como objetivo divulgar a los accionistas e inversionistas, reguladores, bolsas de valores y agencias calificadoras de riesgo, información sobre el desempeño comercial, financiero y operativo de las compañías del grupo y del entorno económico en el cual desarrollan sus actividades.

4.2 POLÍTICA GENERAL DEL MSPI

TGI S.A. ESP buscando establecer un marco de confianza en el ejercicio de operaciones integras, confiables y eficientes, reconoce la importancia de establecer, implementar, mantener y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de proteger sus activos de información (independiente del medio en el que se encuentre), asegurando su disponibilidad, confidencialidad e integridad, enmarcado en la normatividad vigente y aplicable, y alineado con la política y modelo corporativo y pilares para la excelencia.

4.3 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Cada persona entiende su rol para cumplir con las responsabilidades en cuanto a seguridad de la información, apoyándose con los demás miembros de TGI S.A. ESP para lograr los objetivos del MSPI, fomentando el desarrollo de destrezas en un ambiente de aprendizaje continuo.

Por lo anterior, es necesario la definición de Roles con sus correspondientes responsabilidades las cuales se describen en el documento "**Organización Seguridad de la Información TGI**", dando cumplimiento al numeral "5.3 Roles, Responsabilidades y Autoridades en la Organización", y al control asociado: "Roles y responsabilidades para la seguridad de la información" de la norma ISO/IEC 27001:2013.

4.4 DESCRIPCIÓN METODOLÓGICA

A continuación, se realiza la descripción de cada fase que comprende el modelo de seguridad de TGI:

COPIA NO CONTROLADA

4.4.1. Fase 1: Planificación

En esta fase, se establece y se crea el contexto y se realiza el levantamiento del inventario de activos clasificado y etiquetado con el fin de identificarlos para protegerlos de amenazas que afecten la confidencialidad, integridad y disponibilidad de la información.

Durante esta fase se realiza un análisis de todos los riesgos que afectan a los activos identificados. Una vez identificados los riesgos, se deben identificar los controles. El producto generado de esta fase se obtiene de un inventario de activos que está perfectamente estructurado y debe ser el objetivo de actualización permanente, a lo largo de todo el ciclo de vida del Modelo de Seguridad de la Información.

Clasificación de la información: Basados en el contexto de riesgos de seguridad de la información y la metodología de clasificación y etiquetado de la información, el Trabajador, contratista, judicante, practicante, aprendiz SENA y entes de control, buscarán el activo de información en el inventario de activos para validar su clasificación y el etiquetado de información con el fin de proteger los activos de información.

Identificación, valoración y tratamiento de riesgos: El dueño del proceso, actualizará el plan de tratamiento de riesgos y la declaración de aplicabilidad para reflejar el estado de los controles.

Se debe tener en cuenta como aspecto relevante de la gestión de riesgos, que TGI adopta las buenas prácticas propuestas por GEB en cuanto a los riesgos asociados a ciberseguridad:

- Pérdida de la disponibilidad, integridad o confidencialidad de los activos y ciberactivos en operación.
- Pérdida de la confidencialidad, integridad o disponibilidad de los activos de información y/o ciberactivos de la Empresa.

Plan de comunicaciones: Los lineamientos y procedimientos de seguridad de la información se socializarán mediante diferentes mecanismos, para generar cultura organizacional, tales como la generación de un plan de sensibilización de seguridad de la información, que contiene capacitaciones y divulgaciones en temas de seguridad.

4.4.2. Fase 2: Implementación

Una vez identificados los activos se procede a planificar la aplicación de controles propuestos en el plan de tratamiento de riesgos para mitigar las consecuencias que se puedan tener de las amenazas identificadas sobre las vulnerabilidades de los activos.

Implementación del plan de tratamiento de riesgos: Los dueños de los procesos implementarán periódicamente los controles propuestos en el plan de tratamiento de riesgos basados en los planes de tratamiento de riesgos.

Indicadores de gestión: Los dueños de los procesos implementarán y evaluarán periódicamente las métricas e indicadores de gestión de los controles implementados, plan de tratamiento de riesgos y la declaración de aplicabilidad para reflejar el estado de los controles.

Plan de comunicaciones: Los lineamientos y procedimientos de seguridad de la información se socializarán mediante diferentes mecanismos para generar cultura organizacional.

Como parte del plan de tratamiento de riesgos, se define un plan de DRP y se realizan pruebas periódicas con el fin de asegurar la efectividad de la recuperación de los sistemas de información en caso de que ocurra un desastre que afecte la infraestructura tecnológica.

COPIA NO

Se cuenta con una gestión de incidentes de seguridad de la información en la cual se establecen las acciones necesarias para garantizar la identificación, análisis, contención, erradicación y acciones posteriores que sean requeridas con el fin de realizar una atención oportuna a los incidentes de seguridad de la información que se presenten y así minimizar el riesgo de robo o fuga de información.

4.4.3. Fase 3: Evaluación del desempeño

Los dueños de los procesos hacen revisión de la evaluación de los niveles de riesgo residual después de la aplicación de controles y medidas administrativas.

Los dueños de los procesos hacen seguimiento a la programación y ejecución de las actividades de autorías internas y externas.

Hacen medición de los indicadores de gestión de seguridad de la información.

Auditoría debe llevar a cabo auditorías y revisiones planeadas independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de TGI, está implementado adecuadamente y se mantiene de forma eficaz.

4.4.4. Fase 4: Mejora continua

Utilizando los insumos anteriores, los dueños de los procesos pueden efectuar los ajustes a los entregables, controles y procedimientos.

Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección.

La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc., tomadas en sus comités y que impacten el MSPI, plan de tratamiento de riesgos y la declaración de aplicabilidad para reflejar el estado de los controles.

4.4 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se establecen los siguientes principios de seguridad que soportan el MSPI de TGI S.A. ESP:

- **Disponibilidad:** Los activos de información están disponibles cuando se requieran por parte de los usuarios autorizados.
- **Integridad**: Evitar la modificación no autorizada a la información, asegurando su exactitud, completitud y veracidad.
- **Confidencialidad**: Acceso a los activos de información únicamente por los usuarios autorizados.
- **Autenticación**: El acceso a los activos según su nivel de clasificación debe ser concedido a través de mecanismos con diferentes niveles de complejidad, que permita garantizar que quien lo está accediendo es quien dice ser y se encuentra autorizado.
- **Autorización**: A partir de una autenticación exitosa se determina a que recursos puede acceder o usar un usuario a partir de su identidad, los cuales deben ser los mínimos necesarios para el desarrollo de sus funciones.
- **Riesgos de Seguridad de la Información**: Es indispensable una constante Identificación, valoración y tratamiento de riesgos de seguridad de la información asociados a los activos de información y su correspondiente seguimiento para validar el cumplimiento de los planes de tratamiento.

COPIA NO CONTROLADA

- **Cumplimiento normativo**: TGI S.A. ESP cumple con las obligaciones legales, regulatorias y contractuales establecidas en temas de seguridad y privacidad de la información.
- **Responsabilidad:** Todos los trabajadores y demás terceros son responsables de cumplir con las responsabilidades frente a la seguridad de la información.
- **Protección de la Información:** La información generada, procesada o resguardada por los procesos de la operación, la infraestructura tecnológica, las instalaciones de procesamiento, y demás activos de información, se deben proteger de los diferentes riesgos que se puedan presentar, aplicando los controles necesarios de acuerdo con la clasificación de la información.
- **Sistemas de Información Seguros:** Las fases del ciclo de vida de desarrollo o mantenimiento de software incluirán los requisitos de seguridad correspondientes, los cuales deben ser validados y cumplidos antes del paso a producción, y mantenidos durante toda su vida útil.
- **Gestión de eventos e incidentes**: Identificación y reporte oportuno de los eventos e incidentes de seguridad, y las debilidades asociadas de los activos de información, con el fin de dar una respuesta efectiva y oportuna, para mitigar el impacto y poder a partir de las lecciones aprendidas mejorar el MSPI.
- **Auditoria**: Revisión de controles de seguridad para validar que el MSPI esté implementado y mantenido eficazmente.
- **Trazabilidad:** Contar con registros y evidencias que avalen el cumplimiento del MSPI o que a partir de estas se puedan detectar desviaciones o incumplimientos que permitan definir ajustes y mejoras al MSPI.

4.5 INFORMACIÓN DOCUMENTADA

TGI S.A. ESP documenta toda la información necesaria para la conformidad del Modelo de Seguridad y Privacidad de la Información, teniendo en cuenta la normatividad vigente aplicable. De acuerdo con los requisitos a nivel documental que exige la norma ISO 27001:2013, se relacionan a continuación otros documentos que hacen parte del MSPI, así:

- Reglamento de Seguridad de la Información.
- Manual del Sistema de Gestión Integral de Riesgos.
- Formato Gestión de Riesgos de Seguridad de la Información.
- Guía de clasificación y uso aceptable de activos de información.
- Declaración de Aplicabilidad - Controles Anexo A ISO 27001.
- Ficha Indicadores de Seguridad de la Información.
- Normograma Seguridad de la Información.
- Procedimiento Verificación Derechos Autor.
- Procedimiento Recolección Evidencia Digital.
- Procedimiento para la gestión de conexiones remotas.
- Procedimiento para la eliminación segura de información.
- Procedimiento para el trabajo en áreas seguras.
- Procedimiento Instalación de Software en Sistemas Operativos.
- Procedimiento Gestión Roles y Privilegios.
- Procedimiento Gestión Medios Removibles.
- Procedimiento Gestión de Incidentes de Seguridad.
- Procedimiento Gestión Cuentas Usuarios.
- Procedimiento Continuidad Seguridad Información.
- Procedimiento Cifrado.
- Procedimiento Aplicación de Auditorías Internas.
- Instructivo Desarrollo Seguro de Software.
- Contacto con autoridades y grupos de interés.

COPIA NO CONTROLADA