



# **MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**



**We are your Partner  
in Technology**

## ANEXO 6. POLITICAS Y OBJETIVOS DEL SGSI

- Política de Seguridad de la Información
- Política para la Organización de la Seguridad de la Información
- Política para la Clasificación de la información
- Política para el uso aceptable de la información y de los activos asociados
- Política de seguridad en las oficinas - Pantalla y escritorio limpios (En construcción)
- Política de Seguridad en Recursos Humanos
- Política para Seguridad física y ambiental
- Política para la Seguridad en comunicaciones y operaciones
- Política para el Control de Accesos
- Política para los Sistemas de Información
- Política para la Gestión de Incidentes
- Política para la Gestión de la Continuidad
- Política para la Gestión del Cumplimiento

## POLITICA DE SEGURIDAD DE LA INFORMACIÓN

### Objetivo de control SOA: A.5

Para TsTi, la información y el conocimiento son activos de valor estratégico y deben ser gestionados con el propósito de preservar su confidencialidad, integridad y disponibilidad en forma continua.

En TsTi todos somos responsables de la seguridad de la información que generamos, utilizamos, procesamos y accedemos para la prestación de los servicios que entregamos a nuestros clientes. Esta responsabilidad se extiende a nuestras empresas colaboradoras.

Estamos conscientes del valor de la información que administramos y gestionamos. Reconocemos su importancia y principalmente la necesidad de identificar, entender y gestionar los riesgos de nuestro negocio, además de identificar todas las regulaciones en esta materia. En consecuencia, nos ceñimos a los principios básicos en el tratamiento de la información:

- La divulgación de nuestra información de carácter confidencial, así como la divulgación de la información confidencial de nuestros clientes, la consideramos un incumplimiento grave contras las políticas de TsTi y sus accionistas.
- El valor de nuestra información y la de nuestros clientes está en su veracidad, por lo que debemos conservarla en forma íntegra.
- Mantenemos siempre disponible la información más crítica para nuestro negocio y el de nuestros clientes
- La credibilidad de nuestra información y la de nuestros clientes reside en la autenticidad de su fuente, por lo cual desconfiamos de lo anónimo.
- Nuestras tecnologías de información y comunicaciones (TICs) cuentan con medidas de protección y seguridad que aseguran la información contenida en sus componentes.
- El costo de las medidas de seguridad que implementamos es proporcional al valor de la información que protegemos.

La Gerencia General de TsTi, lidera en forma permanente la mejora continua en la Seguridad de la Información de nuestra compañía, así como en los componentes de la infraestructura de TI que ponemos a disposición de nuestros clientes, y asume el compromiso pleno con el Sistema de Gestión de Seguridad de la Información.

## POLÍTICA PARA LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

### Objetivo de control SOA: A.6

**1. OBJETIVO:** Consolidar la gestión de la Seguridad de la Información dentro de TsTi a través de una organización apropiada de las áreas, equipos e individuos asignados a esa función.

**2. ALCANCE :** Definir en forma clara las responsabilidades los roles y responsabilidades para la coordinación y manejo de la seguridad de la información en TsTi

### 3. ROLES Y RESPONSABILIDADES

#### 3.1.COMITÉ DE GERENCIA:

**3.1.1. Definición:** Es el grupo de trabajo conformado por los ejecutivos que representan a la totalidad de la organización.

**3.1.2. Responsabilidades:** El comité busca el compromiso necesario para impulsar los temas estratégicos relacionados a la seguridad de la información en general:

- Conoce el nivel de seguridad de las empresas TsTi a nivel global y aprueba los planes necesarios que desarrollen la función de Seguridad de la Información en Colombia
- Aprueba el Manual de Seguridad de la Información de TsTi
- Aprobar los presupuestos para desarrollar los planes de acción que permitan materializar las estrategias definidas y que permitan madurar en la función de Seguridad de la Información dentro de TsTi
- Designar al Oficial en Jefe/Directivo de alto nivel responsable de la Seguridad de la Información

**3.1.2. Asignación:** Los integrantes del Comité de Gerencia de TsTi son:

GERENCIA GENERAL  
 DIRECCION SERVICIOS COMPARTIDOS  
 DIRECCION COMERCIAL  
 DIRECCIÓN RRHH Y JURIDICA  
 DIRECCION CONTABLE Y FINANCIERA  
 REVISORIA FISCAL  
 DIRECCION SERVICOS TI

### **3.2. OFICIAL EN JEFE DE SEGURIDAD DE LA INFORMACIÓN/DIRECTIVO DE ALTO NIVEL RESPONSABLE**

**3.1.1. Definición:** Es el representante de la Gerencia para la coordinación de las diferentes partes de la organización en lo referente a Seguridad de la Información

**3.1.2. Responsabilidades:** El oficial en jefe de seguridad de la información/directivo de alto nivel responsable busca la cooperación y colaboración de todos los gerentes, administradores, usuarios auditores y personal de seguridad de la información. Tiene la autoridad y la responsabilidad para:

- Conocer la estrategia de Seguridad de la Información de TsTi
- Asegurar que se establecen, implementan y mantienen los controles necesarios para el SGSI
- Asegurarse de promover la toma de conciencia de los requisitos de seguridad de la información en todos los niveles de la organización.
- Informar al Gerente General y al Comité de Gerencia sobre el desempeño del SGSI y de cualquier necesidad de mejora

**3.1.3. Asignación:** La Gerencia General designó a NAYIBERTH FIERRO, Director de Servicios Compartido, como Representante de la Gerencia, Directivo de alto nivel responsable y/o Ejecutivo en Jefe de Seguridad de la Información

### **3.3. COMITÉ COORDINADOR DE SEGURIDAD DE LA INFORMACIÓN**

**3.1.1. Definición:** Es un equipo de trabajo que apoya al Oficial en Jefe de la Seguridad de la Información/Directivo de alto nivel responsable

**3.1.2. Responsabilidades:** El comité busca la relación y trabajo colaborativo que impulse los temas relacionados con la Seguridad de la Información, con un enfoque multidisciplinario. Es responsable por la implementación de los planes y controles de seguridad de la información.

- Ser el asesor especialista en temas de Seguridad de la Información para el Oficial de Seguridad de la Información/Directivo de alto nivel responsable
- Someter a aprobación del Oficial de Seguridad de la Información/Directivo de alto nivel responsable todas las iniciativas de mejora en Seguridad de la Información
- Informar al Gerente General y al Comité de Gerencia sobre el desempeño del SGSI y de cualquier necesidad de mejora
- Analizar los riesgos y las vulnerabilidades de los activos de información de TsTi y de sus Clientes.

- Proponer las medidas tecnológicas y de gestión a implantar para materializar, en los mejores términos de costo y eficacia, la estrategia de Seguridad de la Información de TsTi.
- Colaborar en la elaboración del presupuesto necesario para implementar los controles oportunos para salvaguardar de manera apropiada los activos de información de TsTi y de sus clientes.
- Implementar los proyectos de Seguridad de la Información,
- Informar a las instancias superiores, las incidencias y eventos que se produzcan en TsTi.
- Difundir, entre las unidades de negocio y áreas funcionales, la práctica de Seguridad de la Información
- Trabajar con los Propietarios de Activos de Información, Custodios de Activos de Información y Colaboradores en general para apoyar las actividades de Seguridad de la Información.

**3.1.3. Asignación:** Los integrantes del Comité Coordinador de Seguridad de la Información de TsTi son:

- Gerente General
- Oficial en Jefe de Seguridad Informática
- Consultor de Seguridad Informática
- Líder de SST
- Auditor Líder

## 7. RESPONSABILIDADES

- Director de área: Cumplir las disposiciones de esta política
- Oficial de Seguridad de la Información: Asegurarse de que se establezca la política, se promueva la sensibilización e informar a la Gerencia General sobre su cumplimiento
- Líder SST: Velar por el mantenimiento del presente documento y su posterior actualización. Revisar el cumplimiento de la política por parte de las áreas de la organización.

## 8. DISPOSICIONES FINALES

Vigencia: La presente política entrará en vigencia al momento de ser publicada

Revisión: El contenido de este documento será revisado anualmente o cuando ocurran eventos significativos que requieran su revisión y/o modificación.

\*\*\*\*\* Fin del Documento \*\*\*\*\*