POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

El Gobierno de Seguridad de la Información, en adelante GSI, establece las directrices y lineamientos para planear, implementar, operar, monitorear, revisar, mejorar la seguridad de la información, apoyar la toma de decisiones estratégicas alineados con los objetivos del negocio y el SGSI, con el fin de mitigar los riesgos de seguridad de la información de las compañías del grupo Thomas Greg & Sons, liderando la definición de responsabilidades, la aplicación de buenas prácticas de seguridad de la información y el cumplimiento de los requisitos organizacionales, legales, regulatorios y contractuales; vigentes y relacionados con seguridad de la información, ciberseguridad y privacidad de la información.

El GSI, además contribuye a gestionar el manejo adecuado de la información del grupo Thomas Greg & Sons, quien es consciente del valor de esta y en cumplimiento de su misión, visión y valores corporativos, protege la información propia y de sus clientes, gestionando los riesgos y entorno de amenazas de seguridad de la información asociados y garantizando los principios de:

- ✓ **Confidencialidad**, garantizando el acceso sólo para los usuarios autorizados.
- ✓ **Integridad**, evitando modificaciones no autorizadas.
- ✓ **Disponibilidad**, garantizando que la información esté disponible cuando se necesite.

Razón por la cual la información debe ser protegida en cualquier estado mientras se almacene, procese o transmita, implementando controles, de acuerdo con el impacto que se pueda generar por la divulgación o modificación no autorizada de la misma.

Esta Política es complementada y soportada por políticas específicas, estándares, procedimientos y lineamientos técnicos definidos por el Gobierno de Seguridad de la Información según aplique en las compañías del grupo Thomas Greg & Sons, los cuales establecen los controles y responsabilidades operativas necesarias para su cumplimiento.

ALCANCE

Esta política aplica a todos los trabajadores, activos y/o sistemas de información, infraestructura tecnología, incluyendo servicios en la nube, así como a los procesos o terceros de las compañías del grupo Thomas Greg & Sons, que tengan o puedan tener contacto con los diferentes estados de la información (creación, procesamiento, transmisión y eliminación) propia o bajo su custodia.

OBJETIVO

Implementar, mantener y mejorar en las compañías del grupo Thomas Greg & Sons el GSI, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, alineado con la misión, visión, objetivos del negocio, disposiciones legales, regulatorias,

normativas y contractuales, vigentes, y relacionados con Seguridad de la Información y ciberseguridad, según aplique a cada compañía del grupo Thomas Greg & Sons.

OBJETIVOS ESPECÍFICOS

- ✓ Gestionar los riesgos de seguridad de la información en los procesos que se encuentren dentro del alcance del GSI, alineados a la política de riesgos de cada compañía.
- ✓ Estandarizar el proceso de seguridad de la información que deben cumplir las compañías del grupo Thomas Greg & Sons, según los requerimientos de cada una, mediante la elaboración de políticas y documentos relacionados.
- ✓ Gestionar los incidentes de Seguridad de la Información.
- ✓ Fomentar en los trabajadores y terceros del grupo Thomas Greg & Sons un nivel apropiado de concienciación, madurez y cultura en Seguridad de la Información.
- ✓ Velar que los procesos y sistemas de información cumplan con las políticas y documentos relacionados con seguridad de la información.
- ✓ Cumplir con las obligaciones aplicables y vigentes de tipo legal, regulatorio y contractual relacionadas con la Seguridad de la Información.

NIVEL DE CUMPLIMIENTO

Cualquier trabajador o tercero, que incumpla esta política o las políticas específicas para desarrollar el Gobierno de Seguridad de la Información, debe asumir las responsabilidades y sanciones a que haya lugar, definidas al interior de las compañías del grupo Thomas Greg & Sons, o relacionadas con la normatividad y legislación vigente aplicable a cada compañía.

PRINCIPIOS

- ✓ Cada una de las compañías del grupo Thomas Greg & Sons que este dentro del Gobierno de Seguridad de la Información, debe establecer, implementar, operar, monitorear, revisar, mantener y realizar la mejora continua del SGSI (Sistema de gestión de seguridad de la información) y sus controles aplicables con base en la norma ISO 27001vigente, ley 1581 de 2012 (Protección de datos personales y demás normas aplicables.

- ✓ Las compañías del grupo Thomas Greg & Sons deben establecer y aplicar una metodología documentada para la gestión del riesgo de seguridad de la información, de acuerdo con los requisitos definidos en la política de gestión de riesgos de cada una de las compañías.

- ✓ El Equipo de Seguridad de la Información pondrá en conocimiento de todos los trabajadores o terceros del grupo Thomas Greg & Sons, las políticas de seguridad de la información, sus responsabilidades y deberes pertinentes según el rol desempeñado.

- ✓ Esta política y las que componen el GSI, han sido aprobadas por la alta dirección del grupo Thomas Greg & Sons y están sujetas a una revisión anual.

- ✓ La Alta Dirección del grupo Thomas Greg & Sons demuestra liderazgo y compromiso activo con el Gobierno de Seguridad de la Información, promoviendo el cumplimiento de esta Política y asegurando la disponibilidad de los recursos necesarios para el logro de los objetivos del SGSI.

- ✓ El Equipo de Seguridad de la Información de cada compañía del grupo Thomas Greg & Son debe definir un plan de capacitación anual en "Seguridad de la Información" de acuerdo con las necesidades de cada compañía.

- ✓ Todo trabajador antes de ingresar a trabajar en las compañías del grupo Thomas Greg & Sons, debe contar con un proceso adecuado de selección de personal, para garantizar su idoneidad en el cargo que va a desempeñar.

- ✓ Los procesos de Gestión Humana deben incluir en el proceso de selección y contratación de personal, procedimientos de seguridad antes, durante y después de la contratación.

- ✓ Todo trabajador antes del ingreso a la compañía debe firmar un acuerdo de confidencialidad, el cual debe ser parte integral del contrato.

- ✓ Todo tercero, que en el desarrollo de sus actividades que tenga acceso a información confidencial de las compañías del grupo Thomas Greg & Sons, debe firmar un anexo de seguridad de la información, el cual debe ser parte integral del contrato.

- ✓ Todos los líderes de procesos de las compañías (Gerentes, Directores, Coordinadores, etc.), deben velar por la difusión y cumplimiento de las Políticas de Seguridad de la Información corporativas y de cada compañía al interior de su grupo o equipo de trabajo.

- ✓ Las Directivas del grupo Thomas Greg & Sons reconocen que el Gobierno de Seguridad de la Información forma parte de la cultura organizacional de las compañías, por lo cual se comprometen con el cumplimiento de los objetivos y alcance de GSI, asegurando que los recursos necesarios estén disponibles para ello.

- ✓ Los procesos de las compañías del grupo Thomas Greg & Sons, dueñas de contratos y responsable de las relaciones con terceros, deben velar por la difusión y cumplimiento de las Políticas de Seguridad de la Información corporativas.

- ✓ Conocer y cumplir la política y deberes asociadas al Home Office, según aplique en cada compañía del grupo Thomas Greg & Sons, procurando que se preserve la información a la que se tiene acceso, se procesa o almacena en los lugares donde se realice esta modalidad y protegiendo los principios de seguridad de la información.

- ✓ Se establecen, documentan, implementan y mantienen los requisitos para la seguridad de la información en el proceso de continuidad de negocio, garantizando protección de la información en situaciones adversas.

EXCEPCIONES

Cualquier excepción a la presente Política deberá ser registrada e informada al responsable de la Seguridad de la Información de las compañías del grupo Thomas Greg & Sons que corresponda. Estas excepciones serán analizadas para evaluar el riesgo de seguridad de la información que podrían introducir al grupo Thomas Greg & Sons y, en base a la evaluación de estos riesgos, estos deberán ser asumidos por quien solicita la excepción junto con los lideres o responsables del proceso.