CONTENIDO

1. Introducción

En THOR LTDA, entendemos que la información es un activo estratégico fundamental para la sostenibilidad, competitividad y reputación de la organización. La protección de nuestros datos —tanto internos como de clientes, socios y colaboradores— es una prioridad institucional.

Esta Política de Seguridad de la Información y Ciberseguridad establece el marco normativo que guía la protección de la confidencialidad, integridad, disponibilidad y privacidad (CIA+P) de todos los activos de información de THOR LTDA, así como la gestión proactiva de riesgos cibernéticos en un entorno digital en constante evolución.

Aplica a todos los colaboradores, contratistas, proveedores y cualquier tercero que acceda, utilice o gestione sistemas, redes o información bajo la responsabilidad de THOR LTDA.

Nota: Si bien esta política tiene carácter general, su implementación se adapta a las particularidades operativas, tecnológicas y de riesgo de cada área, siempre bajo los principios de proporcionalidad y eficacia.

2. Objetivos

2.1 Objetivo General

Garantizar la protección integral de los activos de información de THOR LTDA mediante la identificación, evaluación y mitigación de riesgos, la implementación de controles técnicos y organizativos, y la asignación clara de responsabilidades, alineados con la estrategia del negocio y las mejores prácticas internacionales.

2.2 Objetivos Específicos

- Asegurar los principios CIA+P en todos los procesos que involucren información.
- Prevenir, detectar y responder eficazmente a incidentes de seguridad.
- Fomentar una cultura organizacional de seguridad y responsabilidad digital.
- Garantizar la continuidad operativa ante eventos disruptivos.
- Implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con ISO/IEC 27001, NIST CSF y normativa local vigente.

3. Alcance

Esta política aplica a:

- Todo el personal de THOR LTDA (incluyendo altos directivos, gerentes, empleados y contratistas).
- Proveedores, socios tecnológicos y terceros con acceso a sistemas, redes o datos de THOR LTDA.
- Todos los activos de información ya sean físicos, digitales, en la nube, en dispositivos móviles o en medios removibles.

4. Definiciones Clave

Activo de Información	Cualquier dato, sistema, documento o recurso tecnológico con valor para THOR LTDA.
Confidencialidad	Garantía de que la información solo es accesible a personas autorizadas.

Integridad	Precisión, consistencia y confiabilidad de la información a lo largo de su ciclo de vida.
Disponibilidad	Acceso oportuno y confiable a la información cuando sea necesario.
Privacidad	Protección y uso legítimo de datos personales, conforme a la normativa de protección de datos.
Incidente de Seguridad	Evento no deseado que compromete la CIA+P de la información.
SGSI	Sistema de Gestión de Seguridad de la Información.
Área de Tecnología (THOR LTDA)	Unidad responsable de la infraestructura, ciberseguridad y gobernanza tecnológica en THOR LTDA.

5. Normas y Estándares de Referencia

- ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información.
- ISO/IEC 27701:2019 – Extensión para gestión de privacidad.
- Ley 1581 de 2012 (Colombia) – Protección de datos personales.
- Ley 1273 de 2009 – Delitos informáticos.
- NIST Cybersecurity Framework (CSF).
- Buenas prácticas del ENISA y OWASP.

6. Declaración de Compromiso de la Alta Dirección

La Alta Dirección de THOR LTDA reafirma su compromiso con la seguridad de la información mediante:

- El liderazgo visible en la promoción de una cultura de ciberseguridad.

- La asignación de recursos suficientes para la implementación y mantenimiento del SGSI.
- La exigencia de cumplimiento de esta política por parte de todo el ecosistema organizacional.
- La gestión oportuna y transparente de incidentes y riesgos.
- La revisión periódica de esta política para asegurar su vigencia y efectividad.

7. Gobierno y Estructura de Gestión

7.1 Tres Líneas de Defensa

1. Primera Línea: Todos los colaboradores y áreas de negocio — responsables de gestionar riesgos en sus procesos diarios.
2. Segunda Línea: Área de Tecnología (THOR LTDA) — diseña, implementa y monitorea controles de seguridad.
3. Tercera Línea: Auditoría Interna o externa independiente — evalúa la efectividad del marco de gobernanza.

8. Roles y Responsabilidades

DIRECCIÓN	Aprobar la política, definir el apetito de riesgo, asignar recursos y supervisar el desempeño del SGSI.

ÁREA DE TECNOLOGÍA (THOR LTDA)	Implementar controles técnicos, gestionar incidentes, mantener inventarios de activos, capacitar y auditar el cumplimiento.
DIRECTORES DE AREA	Garantizar el cumplimiento en sus equipos, proteger la información bajo su custodia y reportar riesgos.
COLABORADORES	Usar los recursos tecnológicos de forma responsable, proteger sus credenciales, reportar incidentes y participar en capacitaciones.
PROVEEDORES/TERCEROS	Cumplir con los acuerdos de seguridad, confidencialidad y protección de datos establecidos contractualmente.

9. Principios Fundamentales

1. Protección Integral: Aplicar CIA+P en todos los niveles de la organización.

2. Cultura de Seguridad: La ciberseguridad es responsabilidad de todos.

3. Gestión Proactiva de Riesgos: Identificar, evaluar y tratar riesgos al menos una vez al año.

4. Apetito de Riesgo Definido: Aprobado por la Alta Dirección y comunicado a toda la organización.

5. Seguridad por Diseño: Evaluar riesgos en cada cambio tecnológico o proceso nuevo.

6. Monitoreo Continuo: Uso de indicadores (KPIs) y herramientas de detección temprana.

7. Controles Técnicos Robustos: Gestión de accesos, autenticación multifactor (MFA), cifrado, actualizaciones y respaldos.

8. Continuidad del Negocio: Planes de recuperación con componentes de ciberseguridad integrados.

Cumplimiento Legal: Acatar todas las leyes, regulaciones y estándares aplicables.

10. Políticas Operativas Clave

10.1 Clasificación de la Información

La información se clasifica en tres niveles:

- Restringida: Alto impacto si se divulga (ej. datos personales sensibles, secretos comerciales).
- Uso Interno: Solo para empleados de THOR LTDA.
- Pública: Información autorizada para difusión externa.

Los responsables de área deben clasificar y etiquetar sus activos y comunicar dicha clasificación al Área de Tecnología.

10.2 Acceso y Autenticación

- Se aplica el principio de mínimo privilegio.
- Cada usuario debe tener credenciales únicas e intransferibles.
- Contraseñas complejas (mín. 10 caracteres, combinación de mayúsculas, minúsculas, números y símbolos) o, preferiblemente, autenticación multifactor (MFA).
- Bloqueo automático tras 5 intentos fallidos.
- Cambio requerido de clave cada 90 días por Microsoft 365

10.3 Uso Responsable de Recursos Tecnológicos

- Los equipos, redes y sistemas de THOR LTDA son exclusivamente para fines laborales.
- Queda prohibida la instalación de software no autorizado.
- No se permite el almacenamiento de archivos personales (música, videos, juegos, etc.).
- El uso del ancho de banda debe ser eficiente y alineado con las prioridades del negocio.

10.4 Seguridad Física

- Acceso restringido a centros de datos, servidores y áreas críticas.
- Uso obligatorio de sistemas de respaldo (UPS), extintores y mantenimiento preventivo.
- Está prohibido consumir alimentos o bebidas en zonas con equipos tecnológicos sensibles.

10.5 Gestión de Incidentes de Seguridad

- Todo incidente debe reportarse de inmediato al Área de Tecnología.
- Se registrará, investigará y documentará en el sistema centralizado de gestión de incidentes.
- Se aplicarán planes de remediación y se compartirán lecciones aprendidas para prevenir recurrencias.

10.6 Gestión de Proveedores y Terceros

- Todo tercero debe firmar acuerdos de confidencialidad y cumplir con los requisitos de seguridad de THOR LTDA.

- Nunca se deben entregar credenciales directas a proveedores.
- El acceso remoto solo se permite mediante VPN corporativa y con autorización previa.

10.7 Capacitación y Concientización

- Inducción obligatoria en seguridad para nuevos colaboradores.
- Capacitación anual obligatoria con enfoque en phishing, ingeniería social y buenas prácticas.
- Actualizaciones comunicadas vía correo institucional, intranet y campañas de concientización.

11. Tecnologías Emergentes y Riesgos Disruptivos

THOR LTDA adopta tecnologías innovadoras (IA, IoT, automatización, nube, big data) con un enfoque de seguridad desde el diseño. El Área de Tecnología:

- Evalúa riesgos específicos de cada tecnología emergente.
- Implementa controles adaptativos (cifrado, segmentación, monitoreo).
- Incluye escenarios de riesgo disruptivo en los planes de continuidad del negocio.

12. Monitoreo, Evaluación y Mejora Continua

- Evaluación anual de madurez del SGSI según ISO 27001 y NIST CSF.

- Definición y seguimiento de KPIs de seguridad (ej. tiempo de respuesta a incidentes, cumplimiento de parches).
- Revisión y actualización de esta política al menos una vez al año, o ante cambios regulatorios o tecnológicos significativos.

13. Comunicación y Reportes

- Las actualizaciones de la política se comunican vía correo institucional e intranet.
- Reportes consolidados de desempeño en seguridad se presentan trimestralmente a la Alta Dirección.
- La comunicación se realiza en cascada: Área de Tecnología → Gerencias → Equipos.

14. Cumplimiento y Consecuencias por Incumplimiento

El incumplimiento de esta política puede derivar en:

- Medidas disciplinarias (amonestación, suspensión o terminación de contrato).
- Responsabilidad civil o penal, según la gravedad del hecho.
- El desconocimiento de la política no exime de responsabilidad.

15. Administración de la Política

- Responsable de mantenimiento: Área de Tecnología (THOR LTDA)
- Frecuencia de revisión: Anual
- Aprobación final: Alta Dirección de THOR LTDA

- Vigencia: A partir de la fecha de firma

16. Excepciones

Cualquier solicitud de excepción a esta política debe:

- Presentarse por escrito con justificación técnica y de negocio.
- Ser evaluada por el Área de Tecnología.
- Recibir aprobación expresa de la Alta Dirección.
- Incluir controles compensatorios documentados y monitoreados.

JAIRO ANTONIO ASCANIO LOPEZ

Gerente General y Representante Legal