



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Versión: 6

Nivel	Política general (Nivel 1)
Clasificación	USO INTERNO
Propietario del documento	Responsable de Seguridad de la Información (Coordinador de Sistemas)
Fecha de aprobación	2026-06-11
Próxima revisión	Anual o manera extraordinaria ante cambios significativos

ELABORÓ	REVISÓ	APROBÓ
David Castillo	Comité de seguridad de la información	Carlos Moreno Cubillos
Consultor de Sistemas		Director General

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		Código: POL-SI-01
			Versión: 06
			Emisión: 11/06/2026

1. OBJETIVO

Establecer el compromiso y la orientación de la Alta Dirección de TOUREXITO S.A.S. para gestionar la seguridad de la información, definiendo el marco de gobierno bajo el cual se protege la confidencialidad, la integridad y la disponibilidad de la información y de los activos asociados frente a amenazas y daños, de manera que la organización pueda alcanzar sus objetivos de negocio.

Esta política constituye el documento de más alto nivel del Sistema de Gestión de Seguridad de la Información (SGSI). De ella se derivan y con ella deben alinearse y complementarse todas las políticas específicas por tema, procedimientos, normas y controles del sistema, conforme al control 5.1 de la NTC-ISO/IEC 27002:2022.

La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles —incluidas políticas, reglas, procesos, procedimientos y estructuras organizativas— seleccionados a partir de una visión holística y coordinada de los riesgos, dentro de un sistema de gestión coherente.

2. ALCANCE

Esta política aplica a la totalidad del SGSI y es de obligatorio cumplimiento para:

- Todo el personal de la organización, incluyendo empleados directos, temporales, practicantes y contratistas.
- Los proveedores, aliados y terceros que accedan, procesen, almacenen o transmitan información de la organización o de sus clientes.
- Todos los activos de información en cualquier forma (digital, física o verbal) y todos los activos asociados que los soportan: sistemas, aplicaciones, redes, dispositivos, instalaciones y servicios, propios o tercerizados.
- Todas las ubicaciones y modalidades de trabajo, incluidas las instalaciones de la organización, el trabajo remoto y los servicios en la nube.

3. MARCO NORMATIVO Y DE REFERENCIA

Este documento se fundamenta en los siguientes referentes:

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	Código: POL-SI-01
		Versión: 06
		Emisión: 11/06/2026

- NTC-ISO/IEC 27001:2022 — Requisitos del Sistema de Gestión de Seguridad de la Información.
- NTC-ISO/IEC 27002:2022 — Guía para la implementación de controles de seguridad de la información.
- Requisitos legales, reglamentarios, estatutarios y contractuales aplicables a la organización, incluida la normativa colombiana de protección de datos personales (Ley 1581 de 2012 y decretos reglamentarios).
- Ley 1273 de 2009 – Delitos Informáticos (Colombia).
- Objetivos estratégicos, políticas internas y obligaciones contractuales de TOUREXITO S.A.S. con sus clientes y aliados.

4. ROLES Y RESPONSABILIDADES

La Alta Dirección asume la responsabilidad última sobre la seguridad de la información y provee los recursos necesarios para el SGSI. Los roles y responsabilidades se definen y asignan de acuerdo con las necesidades de la organización, estableciendo una estructura definida, aprobada y entendida para la implementación, operación y gestión del sistema.

Rol	Responsabilidades
Alta Dirección (Gerencia General)	• Aprobar la Política General y las políticas específicas del SGSI y proveer los recursos necesarios. • Establecer los criterios de riesgo, y asumir la rendición de cuentas del SGSI. • Promover la cultura de seguridad y revisar el desempeño del sistema (revisión por la dirección).
Comité de Seguridad de la Información	• Dirigir y hacer seguimiento a la implementación del SGSI y aprobar el plan de tratamiento de riesgos. • Resolver conflictos de recursos y priorizar iniciativas de seguridad. • Revisar incidentes significativos, indicadores y resultados de auditoría.
Responsable de Seguridad de la Información	• Elaborar, mantener y proponer la aprobación de las políticas y del marco normativo del SGSI. • Coordinar la gestión de riesgos, la operación de los controles y la gestión de incidentes.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		Código: POL-SI-01
			Versión: 06
			Emisión: 11/06/2026

Rol	Responsabilidades
(Coordinador de sistemas)	Reportar el estado de la seguridad a la Alta Dirección y al Comité.
Propietarios de activos y de riesgos	- Clasificar sus activos de información y aceptar o tratar los riesgos asociados. - Autorizar accesos y velar por el uso adecuado de sus activos.
Líderes de proceso	- Asegurar el cumplimiento de las políticas en sus áreas y asignar responsabilidades operativas. - Apoyar la sensibilización y el proceso disciplinario cuando corresponda.
Todo el personal y terceros	- Conocer, comprender y cumplir las políticas del SGSI aplicables a su rol. - Reportar oportunamente eventos, incidentes y debilidades de seguridad.

4.1. NIVEL DE AUTORIDAD (COMITÉ DE SEGURIDAD DE LA INFORMACIÓN)

El Comité de seguridad tiene máxima autoridad sobre las acciones y recursos relacionados con los temas de seguridad de la información, tiene línea directa con las líneas del negocio y otras áreas de staff o apoyo.

El Comité de Seguridad de la Información se encarga de:

- Actuar como el principal órgano de control para garantizar la implementación operación y gestión de la seguridad de la información dentro de la organización.
- Aprobar y mantener la política de seguridad de la información.
- Garantizar que los objetivos de seguridad de la información cumplan con los parámetros establecidos en el numeral 5 de la presente política.
- Revisar, aprobar, evaluar y priorizar el desempeño de la estrategia de seguridad de la información, con iniciativas tácticas y proyectos que soporten los objetivos de negocio definidos, siempre y cuando se relacionen con la seguridad de la información.
- Asignar las responsabilidades sobre las iniciativas de seguridad, que sean de gran impacto en la organización.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	Código: POL-SI-01
		Versión: 06
		Emisión: 11/06/2026

- Promover el desarrollo de iniciativas que mejoren la cultura organizacional y la conciencia de las partes interesadas y su contribución a la eficacia sobre las medidas de seguridad.
- Evaluar, aprobar o rechazar formalmente las desviaciones a los controles de seguridad, dando cumplimiento a los procedimientos para manejar exenciones y excepciones.
- Evaluar, asignar y controlar los recursos para la implementación de medidas de control de la seguridad de la información con un enfoque claro de costo – beneficio.
- Promover mediante liderazgo y autoridad el cumplimiento de las iniciativas, procesos y procedimientos de seguridad.
- Promover la mejora continua sobre la Seguridad de la Información, mediante la revisión periódica de la gestión realizada.
- Validar el panorama de riesgo de la agencia.
- Analizar y autorizar los niveles permitidos para aceptación del riesgo residual o “tolerancia al riesgo”.
- Validar los reportes de avance de los planes de acción implementados para alcanzar los objetivos de la estrategia de seguridad y su adherencia con respecto a los objetivos de negocio.
- Validar los incidentes y violaciones a esta política, determinando si el incumplimiento se considera "Leve" o "Grave" para la posterior aplicación de medidas disciplinarias.
- Garantizar que existan las directrices necesarias para la "Protección de la información y otros activos asociados".

Periódicamente se debe realizar una valoración del riesgo para contemplar los cambios en los requisitos de seguridad y la situación de riesgo, tales como cambio en los activos, las amenazas, las vulnerabilidades y los impactos. Se debe decidir cuándo un riesgo es aceptable, ya sea por motivos de objetivos de negocio o por costes no rentables. Los posibles tratamientos a los riesgos identificados incluyen:

- Evitar el riesgo.
- Disminuir la probabilidad de ocurrencia.
- Disminuir el impacto.
- Transferir los riesgos.
- Retener los riesgos.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		Código: POL-SI-01
			Versión: 06
			Emisión: 11/06/2026

5. PRINCIPIOS Y DECLARACIONES DE LA POLÍTICA

TOUREXITO S.A.S. declara su compromiso con la protección de la información como un activo esencial para su operación y reputación. Este compromiso se materializa en las siguientes declaraciones de política, que orientan todas las actividades de seguridad de la información:

➤ Definición y objetivos de seguridad de la información

- La seguridad de la información se entiende como la preservación de la confidencialidad (la información es accesible solo a quien está autorizado), la integridad (la información es exacta y completa) y la disponibilidad (la información y los activos están disponibles cuando se requieren), además de propiedades como la autenticidad, la trazabilidad y la no repudiación cuando aplique.
- El objetivo del SGSI es mantener la información y los activos asociados razonablemente seguros y protegidos frente a amenazas y daños, en un nivel de riesgo aceptable para la organización, habilitando el cumplimiento de sus objetivos de negocio.

➤ Compromisos de la organización

- Cumplir los requisitos aplicables de seguridad de la información: los del negocio, los legales, reglamentarios, estatutarios y contractuales.
- Gestionar los riesgos de seguridad de la información mediante un proceso formal, sistemático y repetible de identificación, análisis, evaluación y tratamiento.
- Seleccionar e implementar un conjunto adecuado y coordinado de controles, dentro de un sistema de gestión coherente, para reducir los riesgos a niveles aceptables.
- Mejorar continuamente la idoneidad, adecuación y eficacia del SGSI.

➤ Principios rectores

- Enfoque basado en riesgos: las decisiones de seguridad se sustentan en la evaluación del riesgo y en el valor de los activos para el negocio.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		Código: POL-SI-01
			Versión: 06
			Emisión: 11/06/2026

- Seguridad desde el diseño y por defecto: los requisitos de seguridad se incorporan desde el inicio de los proyectos, servicios y desarrollos, incluyendo el modelado de amenazas y la gestión de vulnerabilidades.
- Menor privilegio y necesidad de conocer: el acceso se concede al mínimo indispensable para el desempeño de las funciones.
- Defensa en profundidad: se combinan controles organizativos, de personas, físicos y tecnológicos en capas complementarias.
- Responsabilidad y rendición de cuentas: cada activo y cada riesgo tiene un propietario definido.
- Resiliencia y continuidad: se prepara a las TIC y a los procesos para mantener la disponibilidad durante interrupciones.

➤ Estructura del cuerpo normativo del SGSI

En un nivel inferior, esta política se apoya en políticas específicas por tema, alineadas y complementarias con ella, que encomiendan la aplicación de los controles. Los temas cubiertos incluyen, entre otros: control de acceso; gestión de activos y uso aceptable; clasificación y tratamiento de la información; seguridad de los recursos humanos; seguridad física y del entorno; configuración segura y dispositivos de usuario final; seguridad de red y transferencia de información; protección contra malware y gestión de vulnerabilidades técnicas; copias de seguridad y redundancia; criptografía y gestión de claves; registro y monitoreo; gestión de incidentes; continuidad del negocio y preparación de las TIC; relaciones con proveedores; desarrollo seguro; y cumplimiento legal y protección de datos personales.

La responsabilidad de la elaboración, revisión y aprobación de cada política específica se asigna al personal pertinente según su nivel de autoridad y competencia técnica. Cuando se modifica una política, se revisan las políticas relacionadas para mantener la coherencia del conjunto.

➤ Manejo de exenciones y excepciones

Toda excepción a las políticas del SGSI debe solicitarse formalmente, justificarse con un análisis de riesgo, documentarse y aprobarse por la autoridad competente, con vigencia temporal y propietario de riesgo asignado.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	Código: POL-SI-01
		Versión: 06
		Emisión: 11/06/2026

6. CONTROLES ISO/IEC 27002:2022 ASOCIADOS

La presente política implementa los siguientes controles del Anexo A de la NTC-ISO/IEC 27001:2022, desarrollados según la guía de la NTC-ISO/IEC 27002:2022:

Control	Nombre del control (ISO/IEC 27002:2022)	Cómo lo aborda esta política
5.1	Políticas de seguridad de la información	Constituye la implementación directa de este control: define la política de nivel superior y el marco de políticas específicas por tema, aprobadas por la dirección, comunicadas y revisadas.
5.2	Roles y responsabilidades de seguridad de la información	Establece la estructura de gobierno y la asignación de roles y responsabilidades del SGSI.
5.4	Responsabilidades de gestión	La dirección exige a todo el personal y terceros aplicar la seguridad de acuerdo con las políticas establecidas.
5.31	Requisitos legales, reglamentarios y contractuales	Declara el compromiso de identificar y cumplir los requisitos aplicables.
5.36	Cumplimiento de las políticas, reglas y normas	Establece la obligatoriedad y la revisión periódica del cumplimiento.

7. EXCEPCIONES, CUMPLIMIENTO E INCUMPLIMIENTO

El cumplimiento de esta política es de carácter obligatorio para todos los destinatarios definidos en el alcance. Su observancia será revisada periódicamente por la función de Seguridad de la Información y por Auditoría Interna, conforme al control 5.36 de la NTC-ISO/IEC 27002:2022, utilizando cuando sea posible herramientas automáticas de medición e informe.

Toda excepción a esta política deberá ser solicitada formalmente, justificada con un análisis de riesgo, documentada y aprobada por el responsable de Seguridad de la Información; las excepciones tendrán vigencia temporal, propietario de riesgo asignado y fecha de revisión. Ninguna excepción podrá comprometer requisitos legales, reglamentarios o contractuales aplicables.

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	Código: POL-SI-01
		Versión: 06
		Emisión: 11/06/2026

El incumplimiento de esta política podrá dar lugar a la aplicación del proceso disciplinario de la organización (Control 6.4), sin perjuicio de las acciones legales o contractuales que correspondan. En caso de detectarse una no conformidad, el Comité de Seguridad de la Información identificará su causa, evaluará y aplicará las acciones correctivas necesarias y verificará su eficacia. Una falta que será sancionada de manera proporcional a su gravedad e impacto, conforme a lo establecido en el reglamento interno de trabajo, y teniendo en cuenta la siguiente escala:

NIVEL	CRITERIO	CONSECUENCIA
Leve	Primer incumplimiento involuntario, sin impacto en la confidencialidad, integridad o disponibilidad de activos de información.	Se aplicarán las sanciones establecidas en el reglamento interno de trabajo, para faltas leves.
Grave	Acción u omisión deliberada que resulte en un incidente de seguridad, fuga de datos, acceso no autorizado a información clasificada o violación de requisitos legales o contractuales.	Se aplicarán las sanciones establecidas en el reglamento interno de trabajo, para faltas Graves.

Una vez informado el incumplimiento, el comité de seguridad de la información, validan lo sucedido y determinan si dicho incumplimiento se considera “Leve” o “Grave”.

Para contratistas y terceros autorizados, el incumplimiento de esta política dará lugar a la revocación inmediata de los accesos otorgados, la activación de las cláusulas de responsabilidad contractual y, cuando corresponda, la terminación anticipada del contrato o acuerdo de servicios.

En todos los casos, el área de Recursos Humanos y el área Jurídica participarán en la evaluación y formalización de las medidas disciplinarias, garantizando el debido proceso y la proporcionalidad de la sanción.

7.1. PROCESO PARA SOLICITAR EXCEPCIONES

Se reconoce que circunstancias operativas excepcionales pueden requerir la desviación temporal de un control de seguridad. En tales casos, se deberá seguir el flujo formal establecido en el Procedimiento de Gestión de Excepciones de Seguridad (PRD-SI-11), cuyas directrices generales son:

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	Código: POL-SI-01
		Versión: 06
		Emisión: 11/06/2026

1. Toda solicitud de excepción deberá ser documentada mediante el formato “Registro de excepciones a la política de seguridad de la información, FOR-SI-05”, indicando la justificación de negocio, el control afectado, los riesgos residuales identificados y los controles compensatorios propuestos.
2. La solicitud deberá contar con la aprobación del líder del área solicitante y la evaluación formal del riesgo por parte del Coordinador de Sistemas.
3. La aprobación final de la excepción corresponde al Comité de Seguridad de la Información o, en su defecto, a la Alta Dirección.
4. Toda excepción aprobada tendrá una vigencia máxima definida, transcurrida la cual deberá ser reevaluada o el control original deberá restablecerse.
5. El Coordinador de Sistemas mantendrá un registro centralizado de todas las excepciones vigentes, el cual será reportado en la revisión por Comité de Seguridad de la Información.

Ningún colaborador, contratista o tercero está autorizado para evadir un control de seguridad sin haber obtenido previamente la aprobación formal a través de este proceso. La evasión no autorizada de un control será tratada como un incumplimiento grave de esta política.

8. REVISIÓN, VIGENCIA Y APROBACIÓN

Esta política será revisada a intervalos planificados, como mínimo una vez al año, o de manera extraordinaria ante cambios significativos en la estrategia del negocio, el entorno técnico, el marco legal o regulatorio, la evolución de riesgos y amenazas, o como resultado de lecciones aprendidas tras un incidente de seguridad de la información.

La política entra en vigor a partir de su fecha de aprobación por la Alta Dirección y permanecerá vigente hasta su modificación o derogación formal. Debe ser comunicada al personal pertinente y a las partes interesadas de forma accesible y comprensible; los destinatarios deben reconocer que la comprenden y se comprometen a cumplirla.

9. CONTROL DE CAMBIOS

VERSIÓN	ÍTEM MODIFICADO	MOTIVO DEL CAMBIO
1		Creación del documento
2	Todo el documento	Se actualiza el documento a la nueva estructura

	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	Código: POL-SI-01
		Versión: 06
		Emisión: 11/06/2026

VERSIÓN	ÍTEM MODIFICADO	MOTIVO DEL CAMBIO
3	Todo el documento	Cambio codificación del documento (Anterior POL-TEI-01)
4	Todo el documento	Se adicionan los siguientes capítulos: Política concientización en materia de seguridad de la información y ciberseguridad Política antimalware Política de seguridad en la red Política de actualización de parches de seguridad Política de gestión de acceso remoto
5	Todo el documento	Se adicionan los siguientes capítulos: Política para la transferencia, almacenamiento y procesamiento de datos con tarjeta de crédito Política de gestión de vulnerabilidades Política para home office Política de RRHH
6	Todo el documento	Se dividen en documentos independientes todas las políticas incluidas en el documento denominado Política de seguridad de la información.