



POLÍTICA DE CUMPLIMIENTO LEGAL, REGLAMENTARIO Y PROTECCIÓN DE DATOS PERSONALES

Versión: 1

Nivel	Política específica por tema (Nivel 2)
Clasificación	USO INTERNO
Propietario del documento	Responsable de Seguridad de la Información (Coordinador de Sistemas)
Fecha de aprobación	2026-02-18
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 DE CUMPLIMIENTO LEGAL, REGLAMENTARIO Y PROTECCIÓN DE DATOS PERSONALES	Código: POL-SI-12
		Versión: 01
		Emisión: 18/02/2026

1. OBJETIVO

Identificar, documentar y cumplir los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información, incluyendo la protección de los datos personales y de los derechos de propiedad intelectual, y asegurar la revisión periódica del cumplimiento del SGSI.

2. ALCANCE

Aplica a todos los procesos, sistemas y personas de la organización sujetos a requisitos legales, reglamentarios o contractuales de seguridad de la información y de protección de datos.

3. MARCO NORMATIVO Y DE REFERENCIA

Este documento se fundamenta en los siguientes referentes:

- Política General de Seguridad de la Información de TOUREXITO S.A.S. (POL-SI-01), con la cual esta política se alinea y complementa.
- NTC-ISO/IEC 27001:2022, Anexo A — Controles de referencia.
- NTC-ISO/IEC 27002:2022 — Guía de implementación de controles.
- Controles 5.31 a 5.36 y 8.34 de la NTC-ISO/IEC 27002:2022.
- Ley 1581 de 2012 y Decreto 1377 de 2013 (Colombia) — Protección de Datos Personales, y demás normativa aplicable.

4. ROLES Y RESPONSABILIDADES

Rol	Responsabilidades
Área Legal	• Identificar y mantener actualizados los requisitos legales y contractuales aplicables.
Oficial/Responsable de Datos Personales	• Velar por el cumplimiento del régimen de protección de datos y atender a los titulares.
Coordinador de sistemas / Auditoría Interna	• Verificar el cumplimiento de las políticas y realizar revisiones independientes.

	POLÍTICA DE CUMPLIMIENTO LEGAL, REGLAMENTARIO Y PROTECCIÓN DE DATOS PERSONALES	Código: POL-SI-12
		Versión: 01
		Emisión: 18/02/2026

5. LINEAMIENTOS DE LA POLÍTICA

➤ Requisitos legales, reglamentarios y contractuales

- Se deben identificar, documentar y mantener actualizados todos los requisitos legales, estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplirlos.
- Estos requisitos deben considerarse en el diseño de los controles y en los acuerdos con terceros.

➤ Propiedad intelectual y registros

- Se deben implementar procedimientos para proteger los derechos de propiedad intelectual y el uso lícito del software y de los materiales protegidos.
- Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso y divulgación no autorizados, conforme a los requisitos legales, reglamentarios, contractuales y del negocio.

➤ Privacidad y protección de datos personales

- La organización debe identificar y cumplir los requisitos de privacidad y protección de la información de identificación personal (PII) según la legislación aplicable, en particular la Ley 1581 de 2012 y sus decretos reglamentarios.
- Se deben aplicar los principios de tratamiento (finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad), obtener autorización cuando corresponda y garantizar los derechos de los titulares.
- Se debe llevar registro de las bases de datos y de las actividades de tratamiento, y notificar los incidentes que comprometan datos personales según lo exija la norma.

➤ Revisión del cumplimiento

- El enfoque de la organización para gestionar la seguridad de la información debe revisarse de forma independiente a intervalos planificados y cuando ocurran cambios significativos.
- El cumplimiento de la política de seguridad, las políticas específicas, las reglas y las normas debe revisarse periódicamente; ante no conformidades, la dirección debe identificar causas y aplicar acciones correctivas.

	POLÍTICA DE CUMPLIMIENTO LEGAL, REGLAMENTARIO Y PROTECCIÓN DE DATOS PERSONALES	Código: POL-SI-12
		Versión: 01
		Emisión: 18/02/2026

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
5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Identifica y documenta los requisitos aplicables.
5.32	Derechos de propiedad intelectual	Protege la propiedad intelectual y el uso lícito del software.
5.33	Protección de registros	Protege los registros según requisitos legales y del negocio.
5.34	Privacidad y protección de PII	Cumple los requisitos de protección de datos personales.
5.35	Revisión independiente de la seguridad de la información	Establece revisiones independientes periódicas.
5.36	Cumplimiento de políticas, reglas y normas	Verifica periódicamente el cumplimiento y las acciones correctivas.

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.

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

	POLÍTICA DE CUMPLIMIENTO LEGAL, REGLAMENTARIO Y PROTECCIÓN DE DATOS PERSONALES	Código: POL-SI-12
		Versión: 01
		Emisión: 18/02/2026

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:

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.

	POLÍTICA DE CUMPLIMIENTO LEGAL, REGLAMENTARIO Y PROTECCIÓN DE DATOS PERSONALES	Código: POL-SI-12
		Versión: 01
		Emisión: 18/02/2026

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	NOMBRE E ITEM MODIFICADO	MOTIVO DEL CAMBIO
1		Creación del documento