
	POLÍTICA SEGURANÇA DA INFORMAÇÃO PARTES INTERESSADAS	Código: PI0029
		Formulário revisado em: 26/08/2025
		N.º Página 1 de 6
		REVISÃO: 00

HISTÓRICO DE REVISÕES DE DOCUMENTOS

REVISÃO	DATA	DESCRIÇÃO
00	27/03/26	<ul style="list-style-type: none"> • Emissão Original.

Elaborador: Mariza Crestani	Consensador: Jean Ribeiro	Aprovador: Ruy Burgos	Publicador: Adelaide Luz
---------------------------------------	-------------------------------------	---------------------------------	------------------------------------

	POLÍTICA SEGURANÇA DA INFORMAÇÃO PARTES INTERESSADAS	Código: PI0029
		Formulário revisado em: 26/08/2025
		N.º Página 2 de 6
		REVISÃO: 00

1. OBJETIVO:

Esta Política tem por objetivo estabelecer diretrizes de Segurança da Informação aplicáveis às partes interessadas externas da TPC, assegurando a proteção das informações e ativos de informação, em conformidade com os requisitos da ISO/IEC 27001, da ISO/IEC 27002 e com o Sistema de Gestão de Segurança da Informação (SGSI) da organização.

Esta política aplica-se a todas as partes interessadas externas que, direta ou indiretamente:

- Acessem informações da organização;
- Utilizem sistemas, redes ou ativos de informação da organização;
- Realizem tratamento de informações em nome da organização.


Inclui, mas não se limita a clientes, fornecedores, parceiros, prestadores de serviço, consultores, terceiros e subcontratados.

2. DOCUMENTOS DE REFERÊNCIA:

- ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação
- ISO/IEC 27002 – Controles de Segurança da Informação
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais ((LGPD)
- Política Interna de Segurança da Informação
- Política de Classificação da Informação
- Política de Controle de Acessos
- Política de Gestão de Incidentes de Segurança da Informação

3. DEFINIÇÕES IMPORTANTES:

TPC: denominação institucional e logomarca utilizada, de forma individual ou conjunta, pelas seguintes empresas do grupo econômico, conforme o contexto de uso: **PRONTO EXPRESS LOGÍSTICA S.A., JSL S.A., INTRALOG LTDA., TPC NORDESTE S.A. e TPC LOGÍSTICA SUDESTE S.A.** Sempre que esta Política fizer referência à “TPC”, tal menção compreenderá a(s) empresa(s) correspondente(s) que utilizem a referida logomarca ou identidade institucional.

	POLÍTICA SEGURANÇA DA INFORMAÇÃO PARTES INTERESSADAS	Código: PI0029
		Formulário revisado em: 26/08/2025
		N.º Página 3 de 6
		REVISÃO: 00

Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da TPC, independente do meio, formato ou localização.

Confidencialidade: garantia que a informação seja acessível **somente a pessoas, entidades ou processos devidamente autorizadas.**

Integridade: garantia que a informação seja **precisa e completa**, e não seja alterada de forma indevida, intencional ou acidental.

Disponibilidade: garantia que a informação e os sistemas estejam acessíveis, **disponíveis quando necessários** pelos usuários autorizados.

Legalidade e conformidade: observância das **leis, regulamentos, normas técnicas, obrigações contratuais e políticas internas aplicáveis.**

Gestão de riscos: processo sistêmico, contínuo e documentado de identificação, análise, avaliação e tratamento de riscos que possam impactar direta ou indiretamente, a segurança das informações ou dos ativos de informação.

4. DIRETRIZES:

4.1. Princípios de Segurança da Informação


A TPC adota os seguintes princípios, alinhados à ISO/IEC 27001:

- **Confidencialidade:** proteção contra acesso, uso ou divulgação não autorizada;
- **Integridade:** proteção contra alteração, destruição ou perda indevida;
- **Disponibilidade:** acesso tempestivo e confiável à informação quando necessário;
- **Legalidade e conformidade:** atendimento aos requisitos legais, regulatórios, contratuais e normativos;
- **Gestão de riscos:** adoção de controles proporcionais aos riscos identificados e avaliados.

4.2. Responsabilidades das Partes Interessadas Externas

As partes interessadas externas devem:

- Cumprir integralmente esta política e demais normas de segurança da informação aplicáveis;

	POLÍTICA SEGURANÇA DA INFORMAÇÃO PARTES INTERESSADAS	Código: PI0029
		Formulário revisado em: 26/08/2025
		N.º Página 4 de 6
		REVISÃO: 00

- Utilizar as informações exclusivamente para as finalidades previamente autorizadas e contratualmente estabelecidos;
- Proteger credenciais de acesso, senhas, certificados e demais mecanismos de autenticação, sendo vedado o compartilhamento;
- Garantir que seus colaboradores, representantes e subcontratados observem requisitos equivalentes de segurança da informação equivalentes;
- Comunicar imediatamente à TPC qualquer incidente, suspeita de incidente ou fragilidades de segurança da informação.

4.3. Classificação, Uso e Proteção da Informação

As informações compartilhadas devem:

- Ser tratadas conforme sua classificação da informação;
- Não ser copiadas, reproduzidas, armazenadas ou transmitidas sem autorização expressa;
- Ser protegidas por controles técnicos e organizacionais adequados, compatíveis com o nível de risco;
- Ser devolvidas ou eliminadas de forma segura e comprovável ao término da relação contratual ou quando solicitado pela TPC.

4.4. Controle de Acesso


O acesso a informações e sistemas:

- Será concedido com base no princípio do **menor privilégio**;
- Dependerá de autorização formal e registrada;
- Poderá ser monitorado, revisado e revogado a qualquer momento;
- Será encerrado imediatamente após o fim da necessidade de negócio ou da relação contratual.

4.5. Proteção de Dados Pessoais

O tratamento de dados pessoais deve:

- Atender integralmente à LGPD e demais legislações aplicáveis;
- Restringir-se às finalidades legítimas, específicas e previamente autorizadas;
- Garantir confidencialidade, integridade e disponibilidade dos dados;

	POLÍTICA SEGURANÇA DA INFORMAÇÃO PARTES INTERESSADAS	Código: PI0029
		Formulário revisado em: 26/08/2025
		N.º Página 5 de 6
		REVISÃO: 00

- Adotadas medidas técnicas e administrativas de proteção dos dados contra acessos não autorizados e incidentes de segurança.

4.6. Gestão de Incidentes de Segurança da Informação

As partes interessadas externas devem:

- Reportar incidentes de segurança da informação imediatamente após sua identificação;
- Cooperar com atividades de investigação, contenção, mitigação e remediação;
- Preservar evidências e informações relevantes, quando solicitado.

4.7. Auditorias e Conformidade

A TPC reserva-se o direito de:

- Avaliar a conformidade com esta política;
- Solicitar evidências de controles de segurança aplicáveis;
- Realizar auditorias, inspeções ou avaliações quando previsto contratualmente.

O não cumprimento poderá resultar em sanções contratuais, suspensão ou revogação de acessos, sem prejuízo de outras medidas cabíveis.

4.8. Exceções

Exceções a esta política devem ser:

- Formalmente solicitadas;
- Avaliadas com base em riscos;
- Aprovadas pela gestão de Segurança da Informação da TPC.


4.9. Revisão e Melhoria Contínua

Esta política é revisada periodicamente ou sempre que houver mudanças relevantes no contexto organizacional, nos riscos, nos requisitos legais ou normativos, como parte do ciclo de melhoria contínua do SGSI, em conformidade com os procedimentos de informação documentada da TPC.

5. RESPONSABILIDADES:

As responsabilidades estão definidas nos subitens do item 4 - Diretrizes.

6. ANEXOS:

	POLÍTICA SEGURANÇA DA INFORMAÇÃO PARTES INTERESSADAS	Código: PI0029
		Formulário revisado em: 26/08/2025
		N.º Página 6 de 6
		REVISÃO: 00

**ANEXO I – TERMO DE COMPROMISSO CONFORMIDADE COM SEGURANÇA
DA INFORMAÇÃO**