

	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO	PSI20/01
	POLÍTICA DE GESTÃO DE SEGURANÇA DE FORNECEDORES	Pág. 1 de 2

1. VISÃO GERAL

- Os fornecedores da Luza Group normalmente não necessitam de acesso físico ou remoto a instalações, sistemas ou infraestruturas em geral. No entanto, quando isso acontece, os princípios estabelecidos nesta política devem ser respeitados.

2. OBJETIVO

- O objetivo desta política é estabelecer diretrizes para os fornecedores da Luza Group sempre que precisarem ter acesso a informações ou dados da Luza Group de qualquer tipo e rede.

3. ABRANGÊNCIA

- Esta política aplica-se ao acesso dos fornecedores da Luza Group à sua infraestrutura ou informação interna, reservada ou confidencial.

4. DESCRIÇÃO

4.1 Generalidades

- O acesso físico a áreas restritas (classificadas com informações reservadas ou confidenciais) exigirá sempre o acompanhamento dos fornecedores por um colaborador da Luza Group.
- O acesso aos servidores da Luza Group para fins de manutenção ou suporte deve ser sempre feito sob supervisão de um membro da Luza Group IT.
- Todos os fornecedores que vão trabalhar nas instalações da Luza Group por um período, devem assinar o termo de confidencialidade e segurança, e responder o R104 - Avaliação de SI para Fornecedores conforme P06 – Gestão de Adm e Compras.
- Os fornecedores são responsáveis por comunicar à Luza Group a ocorrência de eventos ou incidentes de segurança da informação relacionados com a prestação do serviço, ou de que tomem conhecimento durante o mesmo.
- Os fornecedores que necessitem de acesso à rede da Luza Group com equipamento próprio, devem garantir que esta instalou um antivírus atualizado, para limitar o risco de propagação de uma infecção por vírus/malware em toda a infraestrutura.

4.2 Serviços de TI (Externos) - Confidencialidade e Segurança dos Dados

Estabelecer requisitos claros para a gestão de serviços externos de TI é essencial para maximizar os benefícios e mitigar os riscos associados à terceirização de funções críticas de TI. Neste sentido, a empresa deve assegurar que:

- O fornecedor de TI contratado declare (se possível contratualmente) e garanta que não exista nenhum ambiente compartilhado de dados entre os clientes e que cada cliente possui sua própria área segura e isolada dentro dos sistemas e infraestrutura fornecidos. Para grandes fornecedores, como por exemplo as Big Techs, caso não haja esta informação no contrato, deve-se realizar uma pesquisa que comprove o atendimento aos requisitos de segurança e

	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO	PSI20/01
	POLÍTICA DE GESTÃO DE SEGURANÇA DE FORNECEDORES	Pág. 2 de 2

registrar as informações como observação no R11 – IQF – Índice de Qualificação de Fornecedor.

- O fornecedor de TI se comprometa a implementar medidas de segurança adequadas para garantir que os dados da LUZA Group sejam protegidos contra acesso não autorizado, incluindo, mas não se limitando a:
 - ✓ Firewall, criptografia e outras medidas técnicas para proteção dos dados;
 - ✓ Controles de acesso restritos, garantindo que apenas pessoal autorizado da LUZA tenha acesso aos seus dados;
 - ✓ Monitoramento regular dos sistemas para detectar e mitigar quaisquer ameaças à segurança dos dados.
- Em caso de violação das cláusulas contratuais, o fornecedor de TI deverá ser responsável por quaisquer danos resultantes da divulgação não autorizada ou acesso aos dados da LUZA Group, e estará sujeito a medidas legais e compensatórias conforme estipulado em contrato.

5. HISTÓRICO DE REVISÃO

Revisão	Data	Descrição de Alterações
01	10/04/2025	Elaboração do documento.

Autores	
Elaboração	Karolina Lorrane – Especialista da Qualidade
Aprovação	Rafael Ribeiro – Gerente de TI – Global