1. Objetivo

Estabelecer os requisitos mínimos que fornecedores de soluções, serviços e produtos devem atender, a fim de garantir segurança, conformidade, desempenho e integridade dos sistemas e dados da Witzenmann do Brasil.

Este documento está alinhado com normas e legislações reconhecidas, tais como:

- **ISO/IEC 27001** – Segurança da Informação
- **ISO 22301** – Continuidade de Negócios
- **ISO 9001** – Gestão da Qualidade
- **NIST SP 800-53 / SP 800-171** – Controles de Segurança Cibernética
- **LGPD –** Lei Geral de Proteção de Dados (Lei nº 13.709/2018)
- **Diretrizes da ANPD –** Autoridade Nacional de Proteção de Dados

2. Escopo

Aplica-se a todos os fornecedores que prestam serviços ou fornecem produtos a Witzenmann do Brasil.

3. Requisitos Técnicos e de Segurança

3.1 Segurança da Informação

- Os fornecedores devem implementar controles de segurança compatíveis com boas práticas de mercado (ex: ISO/IEC 27001, NIST).
- Devem garantir a proteção de dados contra acessos não autorizados, vazamentos, perda ou corrupção.
- A criptografia deve ser utilizada em repouso e em trânsito, sempre que aplicável.

As cópias impressas/digitais não estão sujeitas a controle de revisão. Versão atual ver no Protheus (p/ docs da WI-BR).

Hardcopies / digital copies are not subject to revision service. Current version see INSIDE (for corporate procedures).

Revisão		Elaborado por		Aprovado por		
Revisão	Data	Depto.	Nome	Depto.	Nome	
00	08/09/2025	TI	Marcos Teixeira	Diretoria	Gilson Barcik	Campo não aplicável na WI-BR Not applicable field at WI-BR
01	09/09/2025	TI	Marcos Teixeira	Diretoria	Gilson Barcik	

Substituto do doc:

3.2 Gestão de Incidentes Cibernéticos

- O fornecedor **deve notificar formalmente a Witzenmann do Brasil em até 24 (vinte e quatro) horas** após a identificação de qualquer incidente de segurança cibernética, incluindo:
    - Ataques de ransomware
    - Vazamento ou comprometimento de dados
    - Invasões ou tentativas de acesso não autorizado
    - Interrupções de serviço causadas por falhas de segurança
- A notificação deve conter:
    - Descrição do incidente
    - Impacto conhecido ou estimado
    - Medidas corretivas adotadas
    - Plano de mitigação e prevenção

3.3 Conformidade Legal e Regulatória

- Os fornecedores devem estar em conformidade com a LGPD (Lei Geral de Proteção de Dados) e demais legislações aplicáveis.
- Devem garantir que qualquer subcontratado também esteja em conformidade com essas exigências.

3.4 Continuidade de Negócios e Recuperação de Desastres

- Devem possuir planos de continuidade de negócios (BCP) e recuperação de desastres (DRP) documentados e testados periodicamente.
- Devem garantir alta disponibilidade e redundância dos serviços críticos.

3.5 Gestão de Acessos

- Acesso aos sistemas e dados da empresa deve ser concedido com base em princípios de mínimo privilégio e necessidade de conhecimento.
- Devem ser utilizados mecanismos de autenticação forte (ex: MFA).

3.6 Monitoramento e Auditoria

- Os fornecedores devem permitir auditorias técnicas e de segurança, mediante aviso prévio.
- Devem manter registros de logs de acesso e atividades, por período mínimo de 30 (trinta) dias.

3.7 Atualizações e Correções

- Softwares e sistemas fornecidos devem ser mantidos atualizados com correções de segurança aplicadas em tempo hábil.
- Vulnerabilidades críticas devem ser tratadas imediatamente após identificação.

3.8 Proporcionalidade

Os requisitos descritos nesta seção, com exceção dos itens 3.2 (Gestão de Incidentes Cibernéticos) e 3.3 (Conformidade Legal e Regulatória), devem ser aplicados de forma proporcional ao tipo de fornecimento, ao nível de criticidade do serviço ou produto contratado e ao impacto potencial sobre os sistemas e dados da Witzenmann.

Fornecimentos pontuais, de baixo risco ou sem integração direta com os sistemas corporativos (exemplo: aquisição de periféricos simples como switches, cabos, adaptadores, entre outros) poderão ser dispensados da aplicação integral desta política, mediante avaliação da área de TI da Witzenmann do Brasil.

4. Avaliação e Desempenho

- O desempenho dos fornecedores será monitorado regularmente com base em indicadores como tempo de resposta, disponibilidade, segurança e conformidade.
- Não conformidades poderão resultar em sanções contratuais, incluindo advertências, penalidades financeiras ou, dependendo da gravidade e impacto das ocorrências, o descredenciamento do fornecedor.

5. Validações Adicionais

Esta política não exclui a realização de verificações e validações adicionais por parte de outros departamentos da Witzenmann do Brasil. Tais validações podem incluir, entre outras:

- Due Diligence
- Sustentabilidade e Responsabilidade Social
- Anticorrupção, Proteção de Dados, Confidencialidade e Sanções
- Treinamento e Conscientização (quando aplicável)

6. Revisão e Atualização

- Este documento será revisado anualmente ou conforme necessidade.
- Alterações serão comunicadas formalmente aos fornecedores.