Política de Segurança da Informação

Confiança, proteção de dados e uso responsável de inteligência artificial

Documento	Classificação	Vigência
Política corporativa e declaração a clientes	Uso controlado	01/05/2026 a 15/04/2027

POSICIONAMENTO A TechFlow AI trata segurança e privacidade como requisitos de projeto. Os controles são definidos de acordo com o risco, a natureza dos dados, o ambiente do cliente e o modelo de prestação do serviço.

Versão 1.1.12 | Criada em 01 de abril de 2026

APROVAÇÃO FORMAL

Lauri Jefferson Miguel — Diretor | Engenharia.

Esta política formaliza compromissos de segurança perante clientes e deve ser acompanhada pela validação periódica dos controles e evidências descritos. A política não constitui certificação ISO, SOC 2 ou garantia absoluta contra incidentes.

Controle do documento

Campo	Definição
Proprietário	TechFlow Artificial Intelligence
Aprovador	Lauri Jefferson Miguel — Diretor | Engenharia
Versão	1.1.12
Periodicidade de revisão	Anual
Canal de segurança	AISecurity@techflowai.com.br
Canal de privacidade / Encarregado	Rhuan@techflowai.com.br
Distribuição	Clientes, prospects, colaboradores, prestadores e parceiros, conforme necessidade

Histórico de versões

Versão	Data	Descrição	Aprovação
1.1.12	01/04/2026	Criação da política integrada de segurança, privacidade, IA e IoT	Lauri Jefferson Miguel

Como interpretar esta política

“Deve” ou “é obrigatório” indica requisito vinculante após a aprovação. “Pode” indica controle dependente do serviço, do risco ou do contrato. Detalhes que poderiam facilitar ataques — como diagramas completos, endereços, regras de detecção e configurações — são fornecidos somente sob confidencialidade e necessidade legítima.

TRANSPARÊNCIA SEM EXPOSIÇÃO A TechFlow disponibiliza evidências proporcionais ao risco e ao estágio da contratação, preservando segredos comerciais, dados de outros clientes e informações que possam enfraquecer a segurança.

Sumário executivo

A TechFlow AI projeta e opera automações, integrações, aplicações com inteligência artificial, soluções de atendimento, software, dispositivos conectados e serviços técnicos. Esta política estabelece um sistema de gestão proporcional ao risco para preservar a confidencialidade, a integridade, a disponibilidade, a privacidade, a autenticidade e o uso responsável das informações.

Compromisso	Aplicação prática
Dados do cliente sob controle do cliente	Uso somente para prestar o serviço, cumprir instruções documentadas e obrigações legais aplicáveis.
Acesso mínimo e rastreável	Identidades individuais, menor privilégio, revisão periódica e registros compatíveis com o risco.
IA com governança	Avaliação de caso de uso, fornecedores, dados, saídas, supervisão humana e riscos próprios de LLMs.
Segurança desde o projeto	Requisitos, revisão, testes e gestão de vulnerabilidades ao longo do ciclo de vida.
Incidentes coordenados	Contenção, investigação, preservação de evidências, comunicação contratual e melhoria.
Responsabilidade compartilhada	Matriz clara entre TechFlow, cliente e provedores para cada solução.

1. Objetivo

Estabelecer princípios, responsabilidades e controles mínimos para proteger informações tratadas pela TechFlow AI e pelas soluções que ela desenvolve, integra, hospeda, configura, mantém ou suporta, promovendo confiança junto a clientes, titulares, colaboradores, fornecedores e demais partes interessadas.

2. Escopo

Aplica-se a pessoas, processos, ambientes, ativos e informações sob gestão ou responsabilidade da TechFlow, inclusive:

- Automações de processos, integrações por API, webhooks, mensageria, CRM, WhatsApp e canais digitais;
- Aplicações de IA generativa, agentes, chatbots, modelos de linguagem, bases de conhecimento, RAG, análise de documentos, voz, imagem e dados;
- Software sob medida, portais, painéis, bancos de dados, repositórios, pipelines e ambientes de desenvolvimento, teste e produção;
- Dispositivos IoT/edge, sensores, câmeras, ESP32, LoRa, telemetria, gateways, firmware, placas, infraestrutura elétrica e serviços em campo;
- Estações de trabalho, identidades, redes, ferramentas corporativas, documentos, código-fonte, credenciais, backups e registros;
- Colaboradores, sócios, terceiros, fornecedores e operadores que tenham acesso a dados ou sistemas no escopo.

Ambientes integralmente administrados pelo cliente permanecem sujeitos também às políticas e controles do cliente. O contrato, a ordem de serviço, o anexo de tratamento de dados e a matriz de responsabilidades podem estabelecer requisitos adicionais.

3. Referências e alinhamento

A política adota abordagem baseada em risco e foi estruturada para ser compatível, sem alegação de certificação, com:

- Lei nº 13.709/2018 (LGPD) e regulamentações/orientações da ANPD;
- ISO/IEC 27001:2022 e práticas da família ISO/IEC 27000;
- NIST Cybersecurity Framework 2.0 e NIST AI Risk Management Framework;
- OWASP Top 10, OWASP API Security Top 10 e riscos de aplicações com LLMs;
- princípios de privacy by design, secure by design, menor privilégio, defesa em profundidade e zero trust.

4. Princípios

Princípio	Diretriz
Confidencialidade	Informação acessível apenas a pessoas, sistemas e organizações autorizadas.
Integridade	Proteção contra alteração, destruição ou processamento indevido.
Disponibilidade e resiliência	Serviços e dados disponíveis conforme criticidade e compromissos acordados.
Privacidade e finalidade	Tratamento legítimo, transparente, mínimo e compatível com a finalidade.
Segurança por padrão e desde o projeto	Controles incorporados ao desenho, configuração e mudança.
Responsabilização	Decisões, acessos, riscos, exceções e incidentes documentados e atribuídos.
Proporcionalidade	Controles ajustados ao risco, criticidade, volume, sensibilidade e contexto.
Supervisão humana	Decisões relevantes apoiadas por IA permanecem sujeitas a revisão apropriada.

5. Governança e responsabilidades

5.1 Diretoria

- Aprovar esta política e prover recursos proporcionais aos riscos;
- Definir apetite a risco, prioridades e responsáveis;
- Receber indicadores, riscos relevantes e lições de incidentes;
- Aprovar exceções de alto risco e aceitar riscos residuais relevantes.

5.2 Responsável por Segurança da Informação

- Manter o programa, o registro de riscos e o plano de tratamento;
- Coordenar controles, conscientização, avaliações, incidentes e revisões;
- Apoiar respostas a clientes e preservar evidências de conformidade;
- Reportar de forma independente riscos materiais à Diretoria.

5.3 Privacidade e proteção de dados

O Encarregado ou função designada orienta a aplicação da LGPD, mantém canais com titulares e ANPD, apoia registros de tratamento, avaliações de impacto e incidentes envolvendo dados pessoais. Os papéis de controlador, operador e operador devem ser definidos por tratamento e contrato, não presumidos de forma genérica.

5.4 Engenharia, operações e atendimento

As equipes devem cumprir requisitos de segurança, manter segregação entre ambientes, proteger segredos, registrar mudanças, tratar vulnerabilidades e escalar eventos.

Ninguém pode contornar controles por conveniência operacional.

5.5 Usuários e terceiros

Toda pessoa com acesso é responsável por credenciais, dispositivos, classificação, uso adequado, confidencialidade e comunicação imediata de suspeitas. Violações podem resultar em revogação de acesso, medidas contratuais e disciplinares cabíveis.

5.6 Segregação de funções

Sempre que viável, desenvolvimento, aprovação, implantação, administração e auditoria são separados. Quando o porte da equipe impedir segregação completa, aplicam-se controles compensatórios como revisão por pares, dupla aprovação, registros imutáveis ou revisão posterior independente.

6. Gestão de riscos e exceções

Riscos são identificados e avaliados antes de novos serviços, integrações, modelos, fornecedores ou mudanças materiais, e reavaliados periodicamente. A análise considera ameaça, vulnerabilidade, probabilidade, impacto, dados envolvidos, dependências, exposição, autonomia da IA e efeitos sobre pessoas e operações.

1. Identificar ativos, fluxos, agentes de tratamento, ameaças, dependências e requisitos.
2. Avaliar risco inerente e controles existentes.
3. Definir tratamento: reduzir, evitar, transferir ou aceitar, com responsável e prazo.
4. Avaliar risco residual, registrar decisão e monitorar o plano.

Exceções devem ter justificativa, escopo, responsável, avaliação de risco, controles compensatórios, prazo de expiração e aprovação proporcional. Exceções não podem ser permanentes por inércia.

7. Inventário, propriedade e classificação da informação

Ativos relevantes devem possuir proprietário, finalidade, localização, classificação, dependências e requisitos de retenção. Fluxos de dados do cliente devem ser documentados em nível suficiente para identificar origem, destino, armazenamento, operadores e transferências.

Classe	Exemplos	Tratamento mínimo
Pública	Conteúdo aprovado para divulgação	Integridade e aprovação de publicação.
Interna	Processos, comunicações e documentação operacional	Acesso autenticado e compartilhamento por necessidade.
Confidencial	Dados de clientes, contratos, código, arquitetura, credenciais indiretas	Menor privilégio, proteção em trânsito/repouso quando aplicável, registro e descarte seguro.
Restrita	Credenciais, chaves privadas, dados sensíveis, biometria, imagens críticas, segredos e dados regulados	Acesso excepcional, proteção reforçada, segregação, monitoramento e proibição em canais não aprovados.

A informação do cliente é classificada no mínimo como Confidencial, salvo se o cliente a tornar pública de forma autorizada. Credenciais e dados pessoais sensíveis são Restritos.

8. Identidade e controle de acesso

- Identidades individuais e proibição de contas compartilhadas, salvo exceção técnica controlada;
- Autenticação multifator para acessos administrativos, remotos, código, nuvem e sistemas que tratem informação Confidencial ou Restrita, quando suportada;
- Menor privilégio, necessidade de conhecer e segregação por cliente/ambiente;
- Aprovação do proprietário para concessão e alteração de acesso;
- Revogação tempestiva em desligamentos, mudança de função, término de contrato ou perda de necessidade;
- Revisões periódicas de acessos privilegiados e relevantes;
- Cofre de segredos para senhas técnicas, tokens e chaves; proibição de segredos em código, tickets, prompts ou mensagens não aprovadas;
- Sessões privilegiadas e ações administrativas registradas conforme risco e capacidade da plataforma.

ACESSO DA TECHFLOW A AMBIENTES DO CLIENTE Deve ser autorizado, limitado ao escopo e período necessários, usar identidade nominativa sempre que possível e respeitar os controles do cliente. Acesso emergencial deve ser registrado e revisado.

9. Criptografia e gestão de segredos

Dados Confidenciais ou Restritos devem ser protegidos em trânsito por protocolos criptográficos atuais e, quando armazenados em ambientes sob gestão da TechFlow, por criptografia compatível com o risco e os recursos da plataforma. Chaves e segredos devem ter acesso restrito, rotação conforme risco ou evento, revogação e separação dos dados protegidos quando tecnicamente possível.

Algoritmos, versões e parâmetros são revistos diante de obsolescência, vulnerabilidade ou exigência contratual. Não se desenvolve criptografia própria para substituir padrões reconhecidos.

10. Segurança de infraestrutura, nuvem e endpoints

- Configuração segura e redução de serviços, portas, permissões e componentes desnecessários;
- Separação lógica de clientes e de ambientes de desenvolvimento, teste e produção;
- Atualizações e correções priorizadas por criticidade, exposição e risco operacional;
- Proteção antimalware/EDR e criptografia de dispositivo quando compatíveis com o endpoint e risco;
- Bloqueio de tela, inventário, gestão de software e proibição de armazenamento local desnecessário;
- Restrição de administração remota, redes confiáveis e canais seguros;
- Backups conforme criticidade, segregados do ambiente primário quando viável e testados periodicamente;
- Capacidade, disponibilidade, alertas e dependências monitorados proporcionalmente ao serviço.

10.1 Trabalho remoto e dispositivos pessoais

Acesso remoto deve usar controles aprovados, MFA e dispositivo adequadamente protegido. O uso de dispositivo pessoal para dados do cliente depende de autorização, separação lógica, atualização, bloqueio, criptografia e possibilidade de remover dados corporativos. Informação Restrita não deve ser armazenada em dispositivos pessoais sem exceção formal.

11. Desenvolvimento seguro e gestão de mudanças

5. Definir requisitos de segurança, privacidade, classificação e responsabilidade antes da implementação.
6. Modelar ameaças para casos de maior risco, incluindo abuso, fraude, prompt injection, vazamento, dependências, APIs e dispositivos.
7. Revisar código e configuração; aplicar análise automatizada quando adequada ao tack e risco.
8. Testar funcionalidade, autorização, tratamento de erros, segregação, logging e cenários de abuso antes da produção.
9. Aprovar e registrar mudanças; manter plano de reversão proporcional ao impacto.
10. Monitorar após a implantação e documentar vulnerabilidades e débitos de segurança.

Dados reais de clientes não devem ser usados em desenvolvimento ou teste sem necessidade, autorização, proteção equivalente e, quando viável, anonimização, pseudonimização ou dados sintéticos. Dependências de software devem ser inventariadas e mantidas; componentes sem suporte ou com risco inaceitável devem ser substituídos ou isolados.

11.1 Vulnerabilidades

Relatos são validados e priorizados considerando severidade técnica, explorabilidade, exposição, dados e impacto. Prazos de correção são definidos por risco e obrigações contratuais. Quando a correção imediata não for segura, aplicam-se mitigação e aceitação formal temporária. Testes invasivos em ambiente do cliente exigem autorização expressa e regras de engajamento.

12. Segurança e governança de inteligência artificial

Soluções de IA devem ser governadas durante todo o ciclo de vida — seleção, concepção, aquisição, configuração, avaliação, implantação, monitoramento e desativação. O uso de IA não reduz as obrigações de segurança, privacidade, qualidade ou responsabilidade profissional.

12.1 Aprovação do caso de uso

Antes do uso produtivo, devem ser identificados finalidade, usuários, dados, modelo/provedor, integrações, nível de autonomia, impacto de erro, supervisão humana, métricas, riscos e forma de interrupção. Casos de alto impacto requerem avaliação e aprovação reforçadas.

12.2 Dados e treinamento

- dados do cliente não devem ser usados para treinar modelos gerais da TechFlow ou de terceiros sem autorização contratual específica e transparente;
- somente provedores e configurações aprovados podem receber dados do cliente;
- prompts, arquivos, embeddings, caches, memória, logs e saídas são tratados conforme sua classificação e finalidade;
- minimização, filtragem, mascaramento, segregação por tenant e prazos de retenção devem ser aplicados conforme o caso;
- fontes de conhecimento devem ter origem, permissão, atualização e escopo de acesso controlados.

12.3 Riscos específicos de LLMs e agentes

Risco	Controles esperados
Prompt injection e conteúdo não confiável	Separar instrução de dados, delimitar ferramentas, validar entradas/saídas, reduzir privilégios e testar ataques.
Vazamento de informação	Filtrar contexto, autorizar por usuário/tenant, evitar segredos em prompts, aplicar DLP/mascaramento quando adequado.
Ações indevidas de agentes	Escopo mínimo, allowlists, limites, confirmação humana para ações sensíveis, idempotência, rollback e kill switch.
Alucinação e erro	Grounding quando apropriado, indicação de incerteza, validação determinística, revisão humana e limites de uso.
Conteúdo nocivo ou enviesado	Políticas de uso, testes representativos, filtros proporcionais, escalonamento e contestação quando aplicável.
Dependência de fornecedor	Avaliação contratual/técnica, monitoramento de mudanças, continuidade e possibilidade de substituição.
Abuso e consumo excessivo	Autenticação, rate limit, cotas, monitoramento, proteção de custos e detecção de anomalias.

12.4 Supervisão e decisões

IA não deve tomar de forma autônoma decisões com efeito jurídico ou impacto material sobre pessoas sem base legal, avaliação apropriada, transparência e salvaguardas. Saídas que influenciem segurança física, saúde, finanças, emprego, crédito, direitos ou operação crítica exigem validação humana qualificada e limites definidos.

12.5 Transparência ao cliente

A TechFlow informa, em nível compatível com o serviço, quando IA é utilizada, qual a finalidade, categorias de dados, principais provedores/suboperadores, limitações relevantes, retenção, controles e responsabilidades. Mudanças materiais em provedor, finalidade ou fluxo devem seguir contrato e processo de mudança.

13. Segurança de IoT, edge, câmeras e sistemas físicos

Soluções conectadas e de campo exigem proteção combinada de hardware, firmware, comunicação, nuvem e operação física.

- identidade única de dispositivo e proibição de credenciais padrão compartilhadas em produção;
- provisionamento seguro, proteção de chaves e desativação/revogação ao fim do ciclo de vida;
- firmware e configurações versionados, com integridade verificada e atualização segura quando suportada;
- interfaces de depuração, portas e serviços desnecessários desabilitados ou fisicamente protegidos;
- segmentação de rede, gateways e regras de comunicação mínimas; dispositivos não devem obter confiança implícita na rede corporativa;
- telemetria minimizada, autenticada e protegida contra alteração e replay conforme risco;
- câmeras e sensores configurados para reduzir coleta, área, resolução, retenção e acesso ao necessário;
- proteção contra adulteração, acesso físico não autorizado, condições ambientais e falhas de energia;
- inventário de versão, localização, proprietário, conectividade, manutenção e descarte de cada ativo relevante;
- modos seguros de falha e operação manual quando a indisponibilidade puder afetar pessoas, ativos ou processos críticos.

SEGURANÇA FÍSICA Nenhuma automação, modelo ou dispositivo deve acionar equipamento com potencial de dano físico sem intertravamentos, limites, teste, supervisão e procedimentos de emergência compatíveis com o risco.

14. Registro, monitoramento e detecção

Sistemas devem gerar registros suficientes para investigar falhas, acessos, mudanças, ações administrativas, integrações e eventos de segurança, respeitando minimização e privacidade. Logs devem ter acesso restrito, proteção contra alteração, sincronização de tempo quando possível e retenção definida por risco, contrato e lei.

Alertas relevantes devem possuir responsável e procedimento de triagem. Conteúdo de prompts e respostas só deve ser registrado quando necessário e autorizado, com filtragem de dados sensíveis sempre que viável. O monitoramento não deve ser usado para vigilância excessiva de pessoas.

15. Gestão de terceiros e operadores

Fornecedores que tratem dados, hospedem serviços, forneçam modelos de IA ou suportem funções críticas são avaliados antes da contratação e periodicamente conforme risco. A avaliação considera segurança, privacidade, localização, retenção, uso para treinamento, subcontratação, resposta a incidentes, continuidade, exclusão, portabilidade e encerramento.

Contratos devem contemplar confidencialidade, finalidade, controles, cooperação, incidentes, auditoria/evidências, devolução ou eliminação e obrigações após o término. A lista de suboperadores aplicável ao serviço deve ser disponibilizada conforme contrato.

16. Proteção de dados pessoais e LGPD

16.1 Papéis e instruções

A TechFlow pode atuar como controladora em suas atividades próprias e como operadora ao tratar dados por conta de clientes. O papel é definido por operação. Como operadora, a TechFlow trata dados conforme instruções documentadas do controlador, salvo obrigação legal aplicável, que será comunicada quando permitido.

16.2 Princípios e direitos

O tratamento deve observar finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização. Solicitações de titulares recebidas como operadora são encaminhadas ao cliente controlador, e a TechFlow presta cooperação razoável para resposta.

16.3 Registros, impacto e transferências

Tratamentos relevantes devem ter finalidade, categorias, agentes, compartilhamentos, retenção, base aplicável e controles registrados. Avaliações de impacto são realizadas quando indicadas pelo risco ou obrigação. Transferências internacionais devem observar mecanismos legais aplicáveis e transparência contratual.

16.4 Retenção e eliminação

Dados são mantidos apenas pelo período necessário à finalidade, contrato, defesa de direitos e obrigações legais. No término, são devolvidos, exportados, anonimizados ou eliminados conforme instrução e viabilidade técnica. Cópias residuais em backups expiram pelo ciclo normal de retenção e permanecem protegidas e indisponíveis para uso corrente.

16.5 Privacidade em imagens, áudio e biometria

Projetos que envolvam câmeras, voz, reconhecimento, biometria ou monitoramento de pessoas exigem avaliação reforçada de necessidade, proporcionalidade, transparência, base legal, acesso, retenção e risco de discriminação. A identificação biométrica não deve ser habilitada por padrão.

17. Continuidade, backup e recuperação

Serviços críticos devem possuir análise de impacto, dependências, estratégia de continuidade e procedimentos de recuperação proporcionais. RTO, RPO, disponibilidade e redundância são definidos por serviço e contrato; não se presumem iguais para todas as soluções.

- testar restauração e procedimentos em periodicidade proporcional ao risco;
- manter contatos, responsabilidades, dependências e prioridades de recuperação;
- prever indisponibilidade de nuvem, APIs, modelos, telecomunicações, energia, dispositivos e pessoas-chave;
- registrar resultados de testes, lacunas e ações corretivas;
- comunicar ao cliente impactos relevantes conforme plano e contrato.

18. Gestão de incidentes de segurança

Suspeitas devem ser comunicadas imediatamente ao canal de segurança. A TechFlow mantém processo para preparação, detecção, triagem, contenção, erradicação, recuperação, preservação de evidências, comunicação e aprendizado.

11. Registrar o evento, horário, origem, escopo inicial e contato responsável.
12. Classificar severidade e acionar equipe técnica, liderança, privacidade, jurídico e cliente conforme necessidade.
13. Conter com segurança, preservar evidências e manter cadeia de custódia proporcional.
14. Investigar causa, dados/sistemas afetados, janela de exposição e impacto provável.
15. Recuperar, monitorar recorrência e validar integridade.
16. Comunicar partes aplicáveis conforme lei e contrato, com fatos confirmados e atualizações úteis.
17. Realizar análise de causa e plano de ação, acompanhando até o encerramento.

NOTIFICAÇÃO AO CLIENTE O prazo e o conteúdo seguem o contrato, a função exercida no tratamento e a legislação aplicável. A comunicação inicial pode ser preliminar e será atualizada à medida que a investigação produzir fatos confiáveis.

19. Pessoas, conscientização e confidencialidade

O acesso depende de compromisso de confidencialidade e treinamento compatível com a função. A conscientização aborda phishing, engenharia social, credenciais, classificação, privacidade, incidentes, IA segura, desenvolvimento e trabalho remoto. Funções privilegiadas ou de alto risco recebem orientação específica.

Processos de admissão, mudança e desligamento devem incluir concessão/revisão/revogação de acesso, devolução de ativos e preservação de informações. Verificações de antecedentes, quando utilizadas, devem ser legais, proporcionais e transparentes.

20. Uso aceitável

É vedado:

- inserir dados de clientes, pessoais, credenciais, código confidencial ou informação Restrita em serviços de IA, armazenamento, tradução ou colaboração não aprovados;
- compartilhar credenciais, desabilitar controles, instalar software não autorizado ou contornar monitoramento;
- acessar dados sem finalidade de trabalho, copiar bases para uso pessoal ou reutilizar dados de um cliente em outro;
- executar varreduras, testes, exploração, captura de tráfego ou engenharia reversa sem autorização;
- usar soluções da TechFlow para fraude, discriminação ilícita, vigilância abusiva, malware, violação de direitos ou atividade ilegal;
- publicar arquitetura, vulnerabilidades, dados, prompts, registros ou detalhes de clientes sem autorização.

21. Segurança física e ambiental

Áreas, equipamentos, protótipos e mídias devem ser protegidos contra acesso, furto, dano e condições ambientais. Visitantes são acompanhados quando necessário. O descarte de equipamentos e mídias deve impedir recuperação razoável dos dados. Trabalho em instalações do cliente segue também as regras locais de segurança física, elétrica, ocupacional e operacional.

22. Auditoria, evidências e melhoria contínua

A efetividade do programa é revisada por indicadores, avaliações, testes, incidentes, vulnerabilidades, feedback de clientes e mudanças no negócio. Não conformidades recebem responsável e prazo. A Diretoria revisa o programa ao menos anualmente.

Indicador mínimo	Objetivo
Cobertura de MFA e acessos revisados	Verificar proteção de identidades e menor privilégio.
Vulnerabilidades por severidade e idade	Controlar exposição e tempo de tratamento.
Incidentes, tempo de triagem/contenção e recorrência	Medir capacidade de resposta e aprendizado.
Restaurações e testes de continuidade	Comprovar recuperabilidade.
Treinamentos e simulações	Reduzir risco humano.
Fornecedores críticos avaliados	Controlar risco da cadeia.
Casos de IA inventariados e avaliados	Manter governança de IA.
Exceções abertas, vencidas e risco residual	Evitar desvios permanentes.

23. Compromissos de transparência com clientes

Mediante solicitação razoável, estágio da contratação, confidencialidade e disponibilidade, a TechFlow pode fornecer evidências adequadas ao risco, como:

- esta política e políticas complementares aplicáveis;
- descrição de arquitetura e fluxo de dados em nível seguro;
- lista de suboperadores e regiões relevantes;
- respostas a questionários de segurança e privacidade;
- resumo de avaliações, testes ou planos de remediação, quando existentes;
- informações sobre retenção, exclusão, backup, continuidade e incidentes;
- matriz de responsabilidades e parâmetros de segurança da solução;
- declaração de inexistência ou status de certificações, sem induzir a erro.

Direito de auditoria, testes independentes, evidências detalhadas, prazos e custos devem ser definidos em contrato. A TechFlow pode oferecer documentação alternativa para evitar exposição de outros clientes ou de controles sensíveis.

24. Responsabilidade compartilhada

Domínio	TechFlow	Cliente
Finalidade e base legal	Implementar o serviço e orientar sobre capacidades/limites.	Definir uso legítimo, público, base legal e instruções.
Acessos	Proteger contas e privilégios sob sua gestão.	Gerir usuários, SSO, permissões e desligamentos sob sua gestão.
Dados	Minimizar, proteger e tratar conforme contrato.	Fornecer dados lícitos, adequados, exatos e classificados.
Integrações	Proteger componentes e credenciais sob gestão da TechFlow.	Configurar sistemas de origem/destino e autorizar escopos.
IA	Configurar salvaguardas e informar limitações.	Definir supervisão, uso permitido e validação das saídas.
Dispositivos	Fornecer configuração/firmware conforme escopo.	Proteger instalação física, rede local, energia e operação.
Incidentes	Investigar e comunicar eventos no escopo TechFlow.	Comunicar suspeitas, preservar evidências e agir no próprio ambiente.
Continuidade	Cumprir níveis contratados e recuperar componentes próprios.	Manter planos para processos e dependências sob sua gestão.

A matriz específica do projeto prevalece quando detalhar responsabilidades adicionais.

25. Violações, exceções e vigência

Descumprimentos devem ser reportados e tratados conforme gravidade, contrato e legislação. Nenhuma retaliação é permitida contra relato de boa-fé. Exceções seguem a Seção 6. Esta política entra em vigor após aprovação formal, é comunicada às partes aplicáveis e revisada no mínimo anualmente.

Anexo A — Declaração de postura de segurança para clientes

USO RECOMENDADO Este anexo pode acompanhar propostas e questionários. Os compromissos gerais estão formalmente aprovados; detalhes técnicos específicos devem ser confirmados no desenho e contrato de cada solução.

Tema	Declaração TechFlow	Como comprovar
Uso dos dados	Uso limitado à prestação do serviço, instruções e obrigações aplicáveis.	Contrato/DPA, fluxo e registro de tratamento.
Treinamento de modelos	Sem uso de dados do cliente para treinamento geral sem autorização específica.	Cláusula contratual e termos do provedor.
Acesso	Menor privilégio, MFA em acessos relevantes e revisão.	Relatório de acessos ou evidência controlada.
Segregação	Separação lógica por cliente e ambiente conforme arquitetura.	Diagrama e teste autorizado.

Tema	Declaração TechFlow	Como comprovar
Criptografia	Proteção em trânsito e repouso conforme risco/plataforma.	Descrição técnica/configuração sob NDA.
Logs	Registros proporcionais para operação e investigação.	Política de logs e amostra saneada.
Desenvolvimento	Requisitos, revisão, testes e gestão de mudanças.	Registros de PR, pipeline e mudanças.
Vulnerabilidades	Priorização por risco, mitigação e rastreamento.	Resumo de varredura/teste e plano.
Incidentes	Processo de resposta e comunicação legal/contratual.	Plano, exercício ou relatório saneado.
Continuidade	RTO/RPO e backup definidos por serviço/contrato.	Plano e evidência de teste.
Suboperadores	Avaliação e transparência conforme contrato.	Lista e cláusulas aplicáveis.
Exclusão	Devolução/eliminação ao término, com ressalva de backup e lei.	Procedimento ou atestado quando contratado.
IA responsável	Inventário, avaliação de risco, supervisão e limites.	Ficha do caso de uso e avaliação.
IoT/edge	Identidade, firmware, rede e proteção física conforme escopo.	Baseline e inventário do projeto.

Anexo B — Evidências recomendadas e plano de prontidão

Para que a política seja defensável em due diligence, a TechFlow deve manter um repositório de evidências. A ausência de um artefato não deve ser ocultada; deve gerar responsável, prioridade e prazo.

Prioridade	Evidência / artefato	Responsável	Status
P0	Aprovação desta política; nomeação dos responsáveis; canais de segurança e privacidade.	Diretoria	[preencher]
P0	Inventário de sistemas, clientes, dados, IA, dispositivos, suboperadores e proprietários.	Segurança/Operações	[preencher]
P0	MFA, revisão de acessos, cofre de segredos e processo de desligamento.	TI/Engenharia	[preencher]
P0	Plano de resposta a incidentes, contatos e exercício de mesa.	Segurança/Diretoria	[preencher]
P0	Templates de DPA, confidencialidade, suboperadores e responsabilidade compartilhada.	Jurídico/Comercial	[preencher]
P1	Baseline de configuração, patching, logs, backup e restauração.	Engenharia/Operações	[preencher]
P1	SDLC seguro, revisão de código, dependências e gestão de vulnerabilidades.	Engenharia	[preencher]
P1	Ficha de avaliação de IA/LLM e testes de prompt injection, vazamento e ações.	IA/Segurança	[preencher]
P1	Baseline IoT/edge, identidade de dispositivo, firmware e desativação.	Hardware/Engenharia	[preencher]
P1	Avaliação de fornecedores críticos e lista pública/contratual de suboperadores.	Compras/Segurança	[preencher]
P2	Testes independentes, varreduras recorrentes e painel de indicadores.	Segurança	[preencher]

Prioridade	Evidência / artefato	Responsável	Status
P2	Roadmap de maturidade e análise de aderência ISO 27001/SOC 2, sem alegar certificação.	Diretoria/Segurança	[preencher]

Anexo C — Checklist de segurança por projeto

Antes da contratação / desenho

- ☐ finalidade, dados, papéis LGPD e classificação definidos
- ☐ arquitetura, fluxos, regiões e suboperadores identificados
- ☐ requisitos do cliente e matriz de responsabilidade acordados
- ☐ risco, continuidade, RTO/RPO e comunicação de incidentes avaliados

Antes da produção

- ☐ MFA, privilégios, segredos e contas de serviço revisados
- ☐ ambientes segregados e dados de teste adequados
- ☐ logs, alertas, backup, restauração e rollback validados
- ☐ vulnerabilidades críticas tratadas e mudança aprovada
- ☐ salvaguardas de IA e/ou IoT testadas quando aplicáveis

Durante a operação

- ☐ acessos, fornecedores, riscos e exceções revisados
- ☐ patches, vulnerabilidades, custos e capacidade monitorados
- ☐ mudanças de modelo, provedor, dados ou finalidade reavaliadas
- ☐ incidentes, falhas e feedback convertidos em melhoria

No encerramento

- ☐ acessos e integrações revogados
- ☐ dados devolvidos/exportados e retenção encerrada
- ☐ dispositivos desprovisionados e segredos revogados
- ☐ eliminação registrada conforme contrato e ciclo de backup
- ☐ documentação e obrigações remanescentes transferidas

Anexo D — Definições

Termo	Definição
Ativo de informação	Informação, sistema, serviço, dispositivo, pessoa ou recurso com valor para a organização.
Controlador	Agente que toma decisões referentes ao tratamento de dados pessoais.
Operador	Agente que trata dados pessoais em nome do controlador.
Suboperador	Terceiro contratado pelo operador para apoiar tratamento realizado em nome do controlador.

Termo	Definição
Incidente de segurança	Evento confirmado que compromete ou pode comprometer confidencialidade, integridade, disponibilidade ou autenticidade.
LLM	Modelo de linguagem de grande escala usado para gerar, classificar ou transformar conteúdo.
RAG	Técnica que recupera conteúdo de fontes autorizadas para compor o contexto de uma IA.
RTO / RPO	Tempo-alvo de recuperação / perda de dados máxima tolerada, definidos por serviço.
DPA	Acordo ou anexo contratual sobre tratamento e proteção de dados.
MFA	Autenticação que exige dois ou mais fatores independentes.

Anexo E — Fontes públicas de referência

- Lei Geral de Proteção de Dados Pessoais — Lei nº 13.709/2018
- ISO/IEC 27001:2022 — Information security management systems
- NIST — Cybersecurity Framework 2.0
- NIST — AI Risk Management Framework
- OWASP — Top 10 for Large Language Model Applications
- OWASP — API Security Top 10

As referências são utilizadas como orientação. A aderência formal, certificação ou conformidade completa depende de avaliação independente, escopo definido e evidências de implementação.

Aprovação

Papel	Nome	Data	Assinatura
Proprietário da política	TechFlow Artificial Intelligence	01/04/2026	
Diretoria / aprovador	Lauri Jefferson Miguel	01/04/2026	gov.br Documento assinado digitalmente LAURI JEFFERSON MIGUEL Data: 20/07/2026 15:23:15-0300 Verifique em https://validar.iti.gov.br
Privacidade / Encarregado	Rhuan Winícyus Kamphorst	01/04/2026	gov.br Documento assinado digitalmente RHUAN WINICYUS KAMPHORST Data: 20/07/2026 15:28:44-0300 Verifique em https://validar.iti.gov.br