

Política de Segurança e Backup

Versão **1.0** · vigente desde a publicação original · B-YOU CREATIVE LTDA · CNPJ 20.947.852/0001-06

Este documento integra o conjunto de documentos oficiais do Ponte para Igrejas e deve ser lido em conjunto com os demais documentos aplicáveis ao serviço. A versão vigente está sempre disponível em ponteparaigrejas.com.br/documentos-legais.

1 Objetivo

Esta Política apresenta as diretrizes gerais de segurança da informação, proteção de dados, controle de acesso, continuidade e backup adotadas no Ponte para Igrejas.

2 Princípios de segurança

O Ponte busca proteger informações de igrejas, usuários, membros, visitantes, crianças, responsáveis, eventos, ministérios, relatórios, registros financeiros e demais dados tratados na plataforma por meio de medidas técnicas e administrativas compatíveis com a natureza do serviço. A segurança depende da atuação conjunta do Ponte, da igreja e dos usuários. O sistema oferece recursos de proteção, mas a igreja precisa configurar permissões corretamente e orientar seus usuários.

3 Infraestrutura

A infraestrutura técnica atualmente prevista para o Ponte utiliza Cloudflare e Supabase, além de provedores e ferramentas necessários para hospedagem, banco de dados, autenticação, armazenamento, segurança, disponibilidade, pagamentos e suporte. O Ponte poderá substituir, complementar ou adicionar fornecedores conforme necessidade técnica, evolução da plataforma, segurança, desempenho ou continuidade do serviço.

4 Controle de acesso

O acesso à plataforma deve ocorrer por credenciais próprias de cada usuário. A igreja deve evitar o compartilhamento de contas e revisar periodicamente quem possui acesso ao sistema. O Ponte utiliza perfil e permissões para limitar o acesso conforme a função de cada pessoa. Dados sensí-

veis, informações de crianças, pedidos privados, dados financeiros e relatórios administrativos devem ser acessados apenas por usuários autorizados.

5 Boas práticas da igreja

A igreja deve manter senhas seguras, remover acessos de pessoas que não atuam mais na organização, revisar permissões de líderes e voluntários, evitar cadastro de dados excessivos, proteger dispositivos utilizados para acessar o sistema e comunicar suspeitas de uso indevido. Usuários não devem salvar senhas em dispositivos compartilhados, encaminhar prints com dados sensíveis sem necessidade, exportar listas sem autorização ou manter cópias desprotegidas de dados pessoais.

6 Registros e auditoria

O Ponte poderá manter registros de acesso, ações relevantes, alterações, logs de segurança, erros e eventos técnicos para prevenção de fraude, investigação de incidentes, suporte, auditoria e melhoria do serviço. Esses registros poderão ser utilizados para identificar uso indevido, orientar a igreja, corrigir falhas e proteger direitos do Ponte, da igreja e dos titulares.

7 Backups e continuidade

O Ponte poderá realizar rotinas de backup, cópias de segurança, redundância ou outras medidas de continuidade compatíveis com a estrutura técnica utilizada. Backups têm finalidade de segurança e recuperação operacional. Eles não substituem a responsabilidade da igreja de manter cópias próprias de informações exportadas quando isso for necessário para sua administração interna, contabilidade, prestação de contas ou obrigação legal.

8 Limites dos backups

A existência de backup não garante recuperação individual de todo registro excluído por usuário autorizado, reversão de alterações feitas pela igreja ou restauração personalizada de informações específicas. Solicitações de recuperação serão avaliadas conforme viabilidade técnica, prazo, escopo, impacto na segurança, integridade dos dados e condições do plano ou suporte aplicável.

9 Incidentes de segurança

Em caso de suspeita de incidente envolvendo dados pessoais ou segurança da plataforma, o Ponte poderá investigar, conter, mitigar impactos, registrar evidências, comunicar a igreja quando necessário e adotar medidas técnicas ou administrativas para reduzir riscos. A igreja deve comuni-

car imediatamente suspeitas de acessos indevidos, senhas comprometidas, exclusões não autorizadas, compartilhamento indevido de dados ou qualquer situação que possa comprometer a segurança da plataforma.

10 Dados sensíveis e crianças

Dados de crianças, adolescentes, saúde, restrições, pedidos de oração, aconselhamento, informações pastorais e dados financeiros exigem atenção reforçada. A igreja deve restringir acessos, orientar usuários e evitar registros desnecessários ou excessivos.

11 Manutenções e atualizações

O Ponte poderá realizar manutenções preventivas, corretivas, emergenciais ou evolutivas. Algumas manutenções podem gerar instabilidade, indisponibilidade temporária ou limitação de acesso. Sempre que possível, mudanças relevantes serão comunicadas de forma adequada, especialmente quando afetarem funcionamento, segurança ou acesso dos usuários.

12 Limitação de responsabilidade

O Ponte não se responsabiliza por incidentes causados exclusivamente por compartilhamento de senhas, dispositivos comprometidos, permissões concedidas incorretamente pela igreja, uso indevido por usuários autorizados, exportações externas desprotegidas ou integrações ativadas sem cuidado adequado. A responsabilidade do Ponte será avaliada conforme sua atuação, documentos aplicáveis, legislação vigente e circunstâncias concretas de cada caso.

13 Contato

Para comunicar suspeitas de segurança ou dúvidas sobre proteção de dados, utilize gestao@ponteparaigrejas.com.br. Para suporte operacional, utilize os canais disponíveis dentro do sistema ou o e-mail contato@ponteparaigrejas.com.br.

B-YOU CREATIVE LTDA · CNPJ 20.947.852/0001-06 · Rua João Vogelsanger, 71, Sala 401 — Joinville/SC
Produto: Ponte para Igrejas · ponteparaigrejas.com.br · contato@ponteparaigrejas.com.br