

PREVENÇÃO E COMBATE À FRAUDE

A **ATZERT ICQ BRASIL ICQ Brasil** está comprometida com a segurança de seus alunos, clientes, parceiros e de seus ambientes digitais.

Esta Política de Prevenção e Combate à Fraude estabelece as diretrizes adotadas pela ATZERT ICQ BRASIL para prevenir, identificar, investigar e responder a possíveis práticas fraudulentas relacionadas ao cadastro de usuários, contratação de cursos, pagamentos, utilização da plataforma, emissão de certificados e demais serviços oferecidos pela empresa.

1. Objetivo

Este documento tem como objetivo estabelecer diretrizes e medidas destinadas à prevenção e ao combate a fraudes e tentativas de fraude, à proteção dos usuários e clientes contra a utilização indevida de seus dados, à segurança dos sistemas e serviços da ATZERT ICQ BRASIL, à redução de riscos relacionados a pagamentos e transações, à prevenção da utilização indevida de contas e credenciais de acesso, bem como à proteção dos conteúdos e certificados disponibilizados pela ATZERT ICQ BRASIL. A Política também busca contribuir para a identificação de comportamentos ou transações potencialmente fraudulentos e estabelecer procedimentos adequados para o tratamento, análise e encaminhamento de situações suspeitas.

2. Abrangência

Este documento aplica-se aos usuários, alunos, clientes, visitantes, parceiros e demais pessoas que utilizem os sites, plataformas, cursos e serviços digitais disponibilizados pela ATZERT ICQ BRASIL ICQ Brasil.

3. O que pode ser considerado fraude

Para fins deste documento, poderão ser consideradas práticas fraudulentas ou potencialmente fraudulentas, entre outras:

- Utilização de identidade ou dados de terceiros sem autorização;
- Criação de contas falsas;
- Fornecimento deliberado de informações falsas;
- Utilização de meios de pagamento de terceiros sem autorização;
- Tentativa de obter serviços mediante fraude;
- Contestação indevida ou fraudulenta de pagamentos;
- Compartilhamento indevido de credenciais;
- Utilização de uma conta por pessoas não autorizadas;
- Tentativa de obter acesso não autorizado à plataforma;
- Manipulação de avaliações, resultados ou registros acadêmicos;
- Falsificação, alteração ou utilização indevida de certificados;
- Cópia ou distribuição não autorizada de materiais dos cursos;
- Utilização de bots, scripts ou mecanismos automatizados para comprometer ou explorar a plataforma;
- Tentativa de burlar mecanismos de segurança;
- Utilização dos serviços para práticas ilícitas;
- Qualquer outra conduta destinada a obter vantagem indevida ou causar prejuízo à ATZERT ICQ Brasil ou a terceiros.

4. Medidas de prevenção

A ATZERT ICQ BRASIL poderá adotar medidas técnicas, administrativas e operacionais destinadas à prevenção de fraudes.

Essas medidas poderão incluir:

- Mecanismos de autenticação;
- Controle de acesso;
- Validação de informações cadastrais;
- Monitoramento de atividades na plataforma;
- Análise de transações;
- Mecanismos de prevenção a pagamentos fraudulentos;
- Identificação de comportamentos anormais;
- Controles relacionados à emissão e validação de certificados;
- Registros de acesso e utilização dos sistemas;
- Mecanismos de segurança da informação;
- Procedimentos internos de investigação.

A adoção de medidas de prevenção poderá ocorrer de forma automatizada ou mediante análise humana, conforme a natureza da situação.

5. Análise de transações

Para proteger usuários e a própria empresa, determinadas transações poderão ser submetidas a mecanismos de análise de risco.

Essa análise poderá considerar informações relacionadas à transação, ao cadastro, ao dispositivo utilizado, ao histórico de utilização e a outros elementos necessários para prevenção de fraude, sempre observadas as bases legais e os direitos previstos na legislação aplicável.

Quando houver indícios relevantes de irregularidade, a ATZERT ICQ BRASIL poderá solicitar informações ou documentos adicionais para confirmação da identidade ou legitimidade da operação.

6. Pagamentos

Os pagamentos poderão ser processados por instituições financeiras, adquirentes, gateways ou outras empresas especializadas.

Esses fornecedores poderão utilizar mecanismos próprios de prevenção a fraudes e realizar verificações necessárias para autorizar ou recusar transações.

A ATZERT ICQ BRASIL poderá receber informações relacionadas ao status da transação e outros dados necessários para confirmar o pagamento e prevenir atividades fraudulentas.

A aprovação ou recusa de uma transação poderá depender de análises realizadas pela ATZERT ICQ BRASIL ou por seus prestadores de serviços de pagamento.

7. Proteção das contas dos usuários

Cada usuário deve manter suas credenciais de acesso sob sua responsabilidade e não deve compartilhá-las com terceiros.

A ATZERT ICQ BRASIL poderá adotar medidas de segurança quando identificar comportamentos incompatíveis com a utilização regular de uma conta.

Quando houver indícios de comprometimento, fraude ou acesso não autorizado, a ATZERT ICQ BRASIL poderá, conforme o caso:

- Solicitar confirmação de identidade;
- Solicitar alteração de senha;
- Bloquear temporariamente determinadas funcionalidades;
- Suspender temporariamente o acesso;
- Realizar análise de segurança;
- Encerrar uma conta quando houver fundamento contratual ou legal.

8. Compartilhamento de credenciais

As credenciais de acesso aos cursos e plataformas são pessoais e, salvo disposição expressa em contrário, não podem ser compartilhadas.

A identificação de utilização incompatível com o padrão normal de uma conta poderá resultar em análise de segurança.

Quando confirmado o uso indevido, poderão ser aplicadas as medidas previstas nos Termos de Uso e nas condições de contratação do curso.

9. Certificados

Os certificados emitidos pela ATZERT ICQ BRASIL poderão possuir mecanismos de identificação, validação ou consulta.

É proibido:

- Falsificar certificados;
- Alterar informações de certificados;
- Utilizar certificado pertencente a outra pessoa;
- Produzir certificados falsos utilizando a identidade visual da atzert icq brasil;
- Comercializar ou distribuir certificados sem autorização;
- Apresentar certificado falso ou adulterado como documento legítimo.

A ATZERT ICQ BRASIL poderá cancelar ou invalidar certificados obtidos mediante fraude ou irregularidade comprovada, observados os procedimentos aplicáveis.

10. Investigação de suspeitas

Quando houver indícios de fraude ou irregularidade, a ATZERT ICQ BRASIL poderá realizar uma investigação interna para compreender os fatos.

A investigação poderá envolver a análise de:

- Registros de acesso;
- Informações cadastrais;
- Histórico de utilização da plataforma;
- Informações relacionadas às transações;
- Registros de autenticação;
- Informações fornecidas pelo próprio usuário;
- Informações recebidas de fornecedores de serviços;
- Outros dados necessários para apuração da situação.

As informações serão utilizadas de acordo com a legislação aplicável e com a Política de Proteção de Dados e Privacidade da ATZERT ICQ BRASIL.

11. Medidas em caso de fraude

Quando houver evidências de fraude ou tentativa de fraude, a ATZERT ICQ BRASIL poderá, conforme a gravidade e as circunstâncias:

- Recusar ou suspender uma transação;
- Bloquear temporariamente uma conta;
- Suspender o acesso a determinados serviços;
- Cancelar uma matrícula quando permitido pelas condições contratuais e pela legislação;
- Invalidar certificados fraudulentos;
- Remover conteúdo ou acessos obtidos irregularmente;
- Exigir comprovação adicional de identidade;
- Preservar registros e evidências;
- Comunicar fornecedores de pagamento;
- Comunicar autoridades competentes quando houver obrigação legal ou quando apropriado;
- Adotar medidas judiciais ou extrajudiciais cabíveis.

As medidas serão adotadas de acordo com a legislação aplicável e considerando as circunstâncias de cada caso.

12. Tratamento de dados pessoais

As medidas de prevenção e combate à fraude podem envolver o tratamento de dados pessoais.

Esse tratamento será realizado de acordo com a legislação aplicável, especialmente a **Lei Geral de Proteção de Dados Pessoais — LGPD**.

Os dados poderão ser utilizados para finalidades como:

- Prevenção e detecção de fraudes;
- Segurança da informação;
- Autenticação;
- Análise de transações;
- Proteção dos usuários;
- Proteção dos sistemas;
- Exercício regular de direitos;
- Cumprimento de obrigações legais ou regulatórias.

Mais informações sobre o tratamento de dados pessoais estão disponíveis na **Política de Proteção de Dados e Privacidade da ATZERT ICQ Brasil**.

13. Comunicação de suspeitas

Caso o usuário identifique uma atividade suspeita, tentativa de fraude, utilização indevida de sua conta ou qualquer incidente relacionado à segurança, deverá comunicar a ATZERT ICQ BRASIL o mais rapidamente possível.

Canal de comunicação:

DPO: Ketley Kemily Silva de Moraes

E-mail: ketley.morais@atzert-icq.com

Ao realizar uma comunicação, recomenda-se informar, quando possível:

- Nome do usuário;
- E-mail cadastrado;
- Descrição do ocorrido;
- Data e horário aproximados;
- Informações sobre a transação, quando aplicável;
- Comprovantes ou evidências relevantes.

14. Responsabilidade do usuário

O usuário deve:

- Fornecer informações verdadeiras;
- Proteger suas credenciais;
- Não compartilhar sua conta;
- Utilizar meios de pagamento de forma legítima;
- Não tentar contornar mecanismos de segurança;
- Não utilizar os serviços para atividades fraudulentas;
- Comunicar imediatamente acessos suspeitos ou não autorizados.

O usuário poderá ser responsabilizado, nos termos da legislação aplicável, por danos decorrentes de condutas fraudulentas ou ilícitas praticadas por ele.

15. Cooperação com autoridades e terceiros

Quando necessário e permitido ou exigido pela legislação, a ATZERT ICQ BRASIL poderá cooperar com instituições financeiras, empresas de pagamento, prestadores de serviços, autoridades policiais, órgãos públicos, autoridades judiciais e demais entidades competentes para prevenção e investigação de fraudes.

Qualquer compartilhamento de dados pessoais será realizado observando as bases legais e demais requisitos previstos na legislação aplicável.

16. Segurança da informação

A ATZERT ICQ BRASIL adota medidas técnicas e administrativas destinadas a proteger seus sistemas e informações contra acessos não autorizados, perda, alteração, destruição ou divulgação indevida.

Nenhum sistema eletrônico, entretanto, pode ser considerado completamente livre de riscos.

Por esse motivo, a colaboração dos usuários é fundamental para a segurança dos serviços.