

POLÍTICA DE CYBERSEGURANÇA

Educpay- Tecnologia e Educação

Última Atualização: 22/12/2024

1. Objetivo

A Política de Cibersegurança da Educpay tem como objetivo garantir a segurança e a integridade de todos os ativos digitais, sistemas, dados e operações internas, bem como assegurar a proteção das informações de clientes e parceiros. Esta política reflete nosso compromisso em adotar as melhores práticas de segurança cibernética, de acordo com os padrões internacionais e regulatórios, visando mitigar riscos e garantir a continuidade dos negócios.

2. Escopo

Esta política aplica-se a todos os colaboradores, terceirizados, fornecedores e parceiros da Educpay, bem como a qualquer pessoa ou entidade que tenha acesso aos sistemas ou dados controlados pela empresa. As regras e diretrizes aqui apresentadas devem ser seguidas no desenvolvimento de software, manutenção de sistemas e na prestação de serviços para clientes de qualquer porte.

3. Princípios de Segurança

A Educpay adota os seguintes princípios como base de sua abordagem à segurança cibernética:

- **Confidencialidade:** Garantir que apenas pessoas autorizadas tenham acesso a informações sensíveis.
- **Integridade:** Proteger os dados contra alterações não autorizadas e garantir sua precisão.
- **Disponibilidade:** Assegurar que os sistemas e serviços estejam disponíveis para uso legítimo de forma contínua.
- **Autenticidade:** Garantir que os dados e as identidades dos usuários sejam verificáveis e confiáveis.

4. Gestão de Acessos

- O acesso aos sistemas e dados da Educpay é baseado no princípio do menor privilégio, onde os usuários recebem apenas as permissões necessárias para realizar suas funções.
- Política de senha aplicada para criação e gerenciamento de senhas de acesso
- Revisões periódicas de permissões de acesso são realizadas para garantir conformidade com os níveis de responsabilidade.
- Registros de atividades dos usuários são monitorados para identificar acessos indevidos ou suspeitos.

5. Classificação e Proteção de Dados

- Todos os dados, incluindo os de clientes, são classificados conforme sua sensibilidade (público, interno, confidencial).
- Informações confidenciais ou sensíveis são criptografadas em repouso e em trânsito.
- A Educpay adota uma política de retenção e descarte seguro de dados, garantindo que informações desnecessárias ou obsoletas sejam eliminadas de forma segura.

6. Desenvolvimento Seguro de Software

A Educpay segue rigorosamente os princípios de Secure Software Development Life Cycle (SDLC), com medidas para garantir que todo software desenvolvido seja resistente a vulnerabilidades cibernéticas:

- Realização de avaliações de segurança durante todas as fases de desenvolvimento, incluindo testes de penetração e análises de código.
- Uso de ferramentas automatizadas de verificação para detectar vulnerabilidades e manter a integridade dos códigos.
- Atualizações contínuas e gerenciamento de patches são aplicados em todos os sistemas, em alinhamento com as melhores práticas e padrões de segurança da indústria.
- Integração com ferramentas de monitoramento para detectar e responder rapidamente a ameaças ou anomalias.

7. Proteção de Infraestrutura e Rede

- Implementação de firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS) e VPNs para proteção das redes da Educpay.
- Asseguramos que todos os dados em trânsito sejam protegidos por protocolos criptográficos robustos.

- Segurança em camadas é aplicada para segmentar as redes e limitar a superfície de ataque.
- Monitoramento contínuo para identificar atividades suspeitas ou tentativas de intrusão.

8. Gestão de Riscos

A Educpay adota uma abordagem pró-ativa na gestão de riscos cibernéticos:

- Conduzimos avaliações periódicas de vulnerabilidades para identificar e corrigir pontos fracos.
- Priorizamos a mitigação dos riscos mais críticos conforme sua probabilidade de ocorrência e impacto potencial.
- Trabalhamos com parceiros de segurança cibernética para garantir uma visão externa e independente dos riscos.

9. Resposta a Incidentes

- A Educpay possui um Plano de Resposta a Incidentes (PRI) robusto, com diretrizes claras sobre como detectar, responder e mitigar o impacto de incidentes cibernéticos.
- Todos os colaboradores recebem treinamento contínuo para reconhecer sinais de ataques e saber como proceder em casos de violação de segurança.
- Incidentes críticos são comunicados imediatamente aos clientes e reguladores relevantes, conforme necessário, e uma investigação detalhada é conduzida para evitar recorrências.

10. Educação e Conscientização

- Todos os colaboradores, desde desenvolvedores a executivos, participam de programas de conscientização e treinamentos regulares em práticas de segurança cibernética.
- Simulações e testes de phishing são realizados periodicamente para garantir que todos estejam preparados para lidar com ataques.
- Encorajamos uma cultura de segurança cibernética na qual todos os membros da equipe reconhecem sua responsabilidade individual em proteger os ativos da empresa e dos clientes.

11. Conformidade com Regulamentações

A Educpay está em conformidade com todas as legislações e regulamentações relevantes de proteção de dados, incluindo, mas não limitado a:

- Lei Geral de Proteção de Dados (LGPD)

- General Data Protection Regulation (GDPR)
- Regulamentos específicos de cada cliente ou setor

Garantimos que todas as práticas de segurança estejam de acordo com as exigências legais para proteger a privacidade e os direitos dos indivíduos cujos dados são processados.

12. Terceirizados e Fornecedores

- Todos os parceiros, fornecedores e terceirizados que têm acesso a sistemas ou dados da Educpay estão sujeitos a avaliações de segurança e devem cumprir com os requisitos desta política.
- Acordos de confidencialidade e contratos com cláusulas de segurança cibernética são exigidos de todas as partes externas envolvidas nos processos da Educpay.

13. Backup e Recuperação de Dados

- Backups regulares são realizados para garantir a proteção dos dados contra perda ou corrupção.
- Todos os backups são armazenados de maneira segura, com criptografia e em locais distintos (on-site e off-site).
- Um plano de recuperação de desastres é mantido e testado periodicamente para garantir a rápida restauração de dados e continuidade dos serviços em caso de falha.

14. Revisão e Atualização da Política

Esta política de cybersegurança é revisada anualmente, ou conforme necessário, para assegurar que continue a atender às necessidades da Educpay e de seus clientes, além de estar em conformidade com as melhores práticas e regulamentações vigentes.

15. Contato

Para dúvidas ou mais informações sobre esta política, entre em contato com o time de segurança cibernética da Educpay pelo e-mail: seguranca@Educpay.com.br.

Educpay- Tecnologia e Educação