Lista de verificação de controles e conformidade

Lista de verificação de avaliação de controles

Sim	Não	Controlar
☐	☑	Menor privilégio
☐	☑	Planos de recuperação de desastres
☐	☑	Políticas de senha
☐	☑	Separação de funções
☑	☐	Firewall
☐	☑	Sistema de detecção de intrusão (IDS)
☐	☑	Cópias de segurança
☑	☐	Software antivírus
☐	☑	Monitoramento, manutenção e intervenção manual para sistemas legados
☐	☑	Criptografia
☐	☐	Sistema de gerenciamento de senha
☑	☐	Fechaduras (escritórios, montra, armazém)
☑	☐	Vigilância em circuito fechado de televisão (CCTV)
☑	☐	Detecção/prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.)

Lista de verificação de conformidade

Padrão de segurança de dados da indústria de cartões de pagamento (PCI DSS)

Sim	Não	Melhores práticas
☐	☑	Somente usuários autorizados têm acesso às informações do cartão de crédito dos clientes.
☐	☑	As informações do cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro.
☐	☑	Implemente procedimentos de criptografia de dados para proteger melhor os dados e pontos de contato de transações de cartão de crédito.
☐	☑	Adote políticas seguras de gerenciamento de senhas.

Regulamento Geral de Proteção de Dados (RGPD)

Sim	Não	Melhores práticas
☑	☐	UE. os dados dos clientes são mantidos privados/protegidos.
☑	☐	Existe um plano em vigor para notificar a E.U. clientes dentro de 72 horas se seus dados forem comprometidos/houver uma violação.
☑	☐	Certifique-se de que os dados sejam devidamente classificados e inventariados.
☑	☐	Aplique políticas, procedimentos e processos de privacidade para documentar e manter os dados adequadamente.

Controles de sistema e organizações (SOC tipo 1, SOC tipo 2)

Sim	Não	Melhores práticas
☐	☑	Políticas de acesso de usuários são estabelecidas.
☐	☑	Dados confidenciais (PII/SPII) são confidenciais/privados.
☐	☑	A integridade dos dados garante que os dados sejam consistentes, completos, precisos e validados.

- [ ] ☑ Os dados estão disponíveis para indivíduos autorizados a acessá-los.

Recomendações (opcional): Alguns padrões podem ser adicionados para melhor segurança dos dados, como: aderir ao PCI DSS para segurança dos dados do cartão de crédito dos clientes, implementar um IDS para identificar e responder rapidamente a ameaças, seguir a regulamentação da GDPR para proteger os dados pessoais visto que a empresa não está em conformidade com os padrões internacionais e dos EUA, usar criptografia para garantir a confidencialidade das informações, privilégio mínimo para que somente alguns funcionários (dependendo do cargo e função) tenha acesso aos dados armazenados, planos de recuperação de desastres e backups diários para evitar perda de dados críticos, colocar uma política de senhas mais rigorosa para maior segurança.