Lista de verificação de controles e conformidade

A Botium Toys:

Lista de verificação de avaliação de controles

Sim	Não	Controle
	x	Privilégio mínimo
	x	Planos de recuperação de desastres
	x	Políticas de senha
	x	Separação de funções
x		Firewall
	x	Sistema de detecção de intrusão (IDS)
	x	Backups
x		Software antivírus
	x	Monitoramento, manutenção e intervenção manual para sistemas legados
	x	Encriptação
	x	Sistema de gerenciamento de senhas
x		Fechaduras (escritórios, vitrine, armazém)
x		Vigilância em circuito fechado de televisão (CCTV)
x		Detecção/prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.)

Lista de verificação de conformidade

Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS)

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

Regulamento Geral de Proteção de Dados (GDPR)

Sim	Não	Prática recomendada
	x	Os dados dos clientes da UE são mantidos privados/seguros.
x		Existe um plano para notificar os clientes da UE dentro de 72 horas se seus dados forem comprometidos/houver uma violação.
	x	Certifique-se de que os dados sejam classificados e inventariados corretamente.
x		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	Prática recomendada
	x	As políticas de acesso do usuário são estabelecidas.
	x	Os dados confidenciais (PII/SPII) são confidenciais/privados.
x		A integridade dos dados garante que os dados sejam consistentes, completos, precisos e tenham sido validados.
	x	Os dados estão disponíveis para indivíduos autorizados a acessá-los.

Recomendações (opcional):

- Implementar a separação de privilégios
- Atribuir privilégios just-in-time
- Agendar backups periódicos para garantir a preservação das informações valiosas.
- Classificar os dados conforme sua importância para priorizar os essenciais.
- Solicitar a troca periódica das senhas cadastradas
- Implementar exigências, como a modificação de pelo menos 3 dígitos da senha
- Proibir o uso de datas de nascimento e o nome do usuário
- Garantir que uma equipe seja responsável por realizar o monitoramento de todos os acessos

- Implantar o IDS fora da banda, em modo de escuta, para analisar todo o tráfego.
- Utilizar encriptação e gerenciadores de senhas.