Lista de verificação de controles e conformidade

Lista de verificação de avaliação de controles

Sim	Não	Controle
	●	Menor Privilégio
	●	Planos de recuperação de desastres
	●	Políticas de senha
●		Separação de funções
●		Firewall
	●	Sistema de detecção de intrusão (IDS)
		Backups
●		Software antivírus
	●	Monitoramento manual, manutenção e intervenção para sistemas legados
	●	Criptografia
	●	Sistema de gerenciamento de senhas
●		Fechaduras (escritórios, vitrines, armazéns)
●		Vigilância por circuito fechado de televisão (CFTV)
●		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 pontos de contato e os dados das transações com cartão de crédito.
		● Adote políticas seguras de gerenciamento de senhas.

Regulamento Geral de Proteção de Dados (RGPD)

Sim	Não	Melhores práticas
		Os dados dos clientes da U.E. são mantidos privados/seguros.
●		Existe um plano para notificar os clientes da U.E. dentro de 72 horas se seus dados forem comprometidos/houver uma violação.
		Garanta que os dados sejam classificados e inventariados adequadamente.
●		Aplique políticas, procedimentos e processos de privacidade para documentar e manter dados adequadamente.

Controles de Sistemas e Organizações (SOC tipo 1, SOC tipo 2)

Sim	Não	Melhores práticas
		Políticas de acesso do usuário são estabelecidas.
		● Dados sensíveis (PII/SPII) são confidenciais/privados.
		A integridade dos dados garante que os dados sejam consistentes, completos, precisos e tenham sido validados.

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

Esta seção é opcional e pode ser usada para fornecer um resumo de recomendações ao gerente de TI sobre quais controles e/ou práticas recomendadas de conformidade a Botium Toys precisa implementar, com base no risco representado se não forem implementados em tempo hábil.

Recomendações (opcional):

Recomendo de forma urgente a adoção das seguintes medidas para sanar todas as brechas de segurança.

Controle Preventivo:

Menor privilégio - Os usuários só terão acesso no que for necessário ao que suas funções determinarem.

Políticas de senhas - Implementação de políticas de senhas complexas para reduzir as chances de comprometimento de contas, risco de um ataque de força bruta ou de dicionário.

Monitoramento, manutenção e intervenção manual - Necessário para identificar e gerenciar ameaças, riscos ou vulnerabilidades em sistemas desatualizados.

Controle Corretivo:

Plano de recuperação de desastre - A empresa não conta com um plano de recuperação de desastres. Necessário implementar.

Backup - Necessário implementar uma política diária de backups.