Checklist de controles e compliance

A partir da análise do escopo, das metas e do relatório de avaliação de risco presente em: Botium Toys: Scope, goals, and risk assessment report, será realizada uma auditoria interna a partir do preenchimento de uma lista de verificação de controles e conformidade.

Checklist de avaliação de controles

Sim	Não	Controle
☐	☑	Menor privilégio
☐	☑	Planos de recuperação de desastres
☐	☑	Políticas de senhas
☐	☑	Separação de funções
☑	☐	Firewall
☐	☑	Sistema de detecção de intrusão (SDI)
☐	☑	Backups
☑	☐	Software antivirus
☐	☑	Monitoramento de manual, manutenção e intervenção para sistemas legados
☐	☑	Criptografia
☐	☑	Sistema de gerenciamento de senhas
☑	☐	Fechaduras (escritórios, fachadas de lojas, depósitos)
☑	☐	Vigilância por circuito fechado
☑	☐	Detecção/prevenção de incêndio

Checklist de compliance

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

Sim	Não	Melhor prática
☐	☑	Apenas usuários autorizados têm acesso às informações de cartão de crédito dos clientes.
☐	☑	As informações de cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro.
☐	☑	Implementar procedimentos de criptografia de dados para proteger melhor os pontos de contato e os dados das transações com cartão de crédito.
☐	☑	Adotar políticas seguras de gerenciamento de senhas.

Regulamento geral sobre a proteção de dados (GDPR)

Sim	Não	Melhor prática
☐	☑	Os dados dos clientes são mantidos privados e seguros.
☑	☐	Existe um plano em vigor para notificar os clientes em até 72 horas se os seus dados forem comprometidos ou se houver alguma violação.
☐	☑	Garantir que os dados sejam classificados e inventariados adequadamente.
☑	☐	Aplicar políticas, procedimentos e processos de privacidade para documentar e manter os dados adequadamente.

Controles de sistemas e organizações (SOC 1/2)

Sim	Não	Melhor prática

☐	☑	As 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 validados.
☐	☑	Os dados estão disponíveis para indivíduos autorizados a acessá-los.

Recomendações: É notório que a organização deixa a desejar em diversos aspectos relacionados à segurança, visto que é urgentemente necessário implementar controles como delimitação de acesso por funções, políticas de senha, backups, sistemas de detecção de intrusão e criptografia de dados.

No que tange ao compliance da empresa, existe um déficit enorme que pode representar riscos diretos à segurança e gerar multas para a organização. Para que isso seja resolvido, é necessário aplicar os controles de segurança descritos acima e as boas práticas relacionadas a segurança de dados e compliance.