Checklist Controle de Segurança

Para completar a lista de verificação de avaliação de controles, consulte as informações fornecidas no relatório de escopo, metas e avaliação de risco. Para mais detalhes sobre cada controle, incluindo o tipo e a finalidade, consulte o documento de categorias de controle.

Em seguida, selecione "sim" ou "não" para responder à pergunta: A Botium Toys atualmente possui esse controle implementado?

Lista de verificação de avaliação de controles

Sim	Não	Controle
☐	☑	Menor previlégio
☑	☐	Planos de Recuperação de Desastres
☐	☑	Politica de senhas
☑	☐	Separação de Funções
☑	☐	Firewall
☐	☑	Sistema de Detecção de Intrusão (IDS)
☐	☑	Backups
☑	☐	Software Antivírus
☑	☐	Monitoramento, Manutenção e Intervenção Manual para Sistemas Legados
☐	☑	Criptografia
☐	☑	Sistema de Gerenciamento de Senhas
☑	☐	Trancas (escritórios, loja, armazém)
☑	☐	Vigilância por Circuito Fechado de Televisão (CCTV)

☑	☐	Detecção/Prevenção de Incêndios (alarme de incêndio, sistema de sprinklers, etc.)

Para completar a lista de verificação de conformidade, consulte as informações fornecidas no relatório de escopo, metas e avaliação de risco. Para mais detalhes sobre cada regulamento de conformidade, revise os controles, frameworks e leituras sobre conformidade.

Em seguida, selecione "sim" ou "não" para responder à pergunta: A Botium Toys atualmente adere a esta prática recomendada de conformidade?

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 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 melhor proteger os pontos de contato e os dados das transações com cartão de crédito.
☐	☑	Adotar políticas seguras de gerenciamento de senhas.

Regulamento Geral de Proteção de Dados (GDPR)

Sim	Não	Melhores práticas
☑	☐	Os dados dos clientes da E.U. são mantidos privados/seguros.
☑	☐	Há um plano em vigor para notificar os clientes da E.U. dentro de 72

		horas se seus dados forem comprometidos/houver uma violação.
☑	☐	Garantir que os dados sejam devidamente classificados e inventariados.
☑	☐	Reforçar políticas, procedimentos e processos de privacidade para documentar e manter corretamente os dados.

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

Sim	Não	Melhores práticas
☐	☑	Políticas de acesso de usuários estão 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.

Recomendações: Para fortalecer a segurança da Botium Toys, recomendamos a implementação de criptografia robusta para proteger dados sensíveis, incluindo informações de cartões de crédito e dados pessoais identificáveis. É crucial estabelecer controles de acesso rigorosos, baseados no princípio do menor privilégio e na separação de funções. Além disso, a instalação de um sistema de detecção de intrusão (IDS) ajudará a monitorar e identificar atividades suspeitas.

Desenvolva e mantenha um plano de recuperação de desastres, incluindo backup e recuperação de dados essenciais. Adote um sistema de gerenciamento centralizado de senhas com políticas de segurança robustas. Realize auditorias de segurança regulares e implemente treinamento contínuo para todos os funcionários, aumentando

a conscientização sobre práticas de segurança. Atualize as políticas de segurança para refletir mudanças nas regulamentações e nas melhores práticas, garantindo também a conformidade com regulamentações internacionais, como o GDPR.