

Lista de verificação de controles e conformidade

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

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

Lista de verificação de avaliação de controles

Sim	Não	Controlar
<input type="checkbox"/>	<input type="checkbox"/>	Menor Privilégio
<input type="checkbox"/>	<input type="checkbox"/>	Planos de recuperação de desastres
<input type="checkbox"/>	<input type="checkbox"/>	Políticas de senha
<input type="checkbox"/>	<input type="checkbox"/>	Separação de funções
<input type="checkbox"/>	<input type="checkbox"/>	Firewall
<input type="checkbox"/>	<input type="checkbox"/>	Sistema de detecção de intrusão (IDS)
<input type="checkbox"/>	<input type="checkbox"/>	Backups
<input type="checkbox"/>	<input type="checkbox"/>	Software antivírus
<input type="checkbox"/>	<input type="checkbox"/>	Monitoramento manual, manutenção e intervenção para sistemas legados
<input type="checkbox"/>	<input type="checkbox"/>	Criptografia
<input type="checkbox"/>	<input type="checkbox"/>	Sistema de gerenciamento de senhas
<input type="checkbox"/>	<input type="checkbox"/>	Fechaduras (escritórios, vitrines, armazéns)

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | Vigilância por circuito fechado de televisão (CFTV) |
| <input type="checkbox"/> | <input type="checkbox"/> | Detecção/prevenção de incêndio (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 riscos](#). Para mais detalhes sobre cada regulamentação de conformidade, revise a leitura [controles, estruturas e conformidade](#)

Em seguida, selecione “sim” ou “não” para responder à pergunta: *A Botium Toys atualmente adere a esta melhor prática de conformidade?*

Lista de verificação de conformidade

Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS)

- | Sim | Não | Melhores práticas |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | Somente usuários autorizados têm acesso às informações do cartão de crédito dos clientes. |
| <input type="checkbox"/> | <input type="checkbox"/> | As informações do cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro. |
| <input type="checkbox"/> | <input type="checkbox"/> | Implemente procedimentos de criptografia de dados para proteger melhor os pontos de contato e os dados das transações com cartão de crédito. |
| <input type="checkbox"/> | <input type="checkbox"/> | Adote políticas seguras de gerenciamento de senhas. |

Regulamento Geral de Proteção de Dados (RGPD)

- | Sim | Não | Melhores práticas |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | Os dados dos clientes da U.E. são mantidos privados/seguros. |

- | | | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | Existe um plano para notificar os clientes da U.E. dentro de 72 horas se seus dados forem comprometidos/houver uma violação. |
| <input type="checkbox"/> | <input type="checkbox"/> | Garanta que os dados sejam classificados e inventariados adequadamente. |
| <input type="checkbox"/> | <input type="checkbox"/> | 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
------------	------------	--------------------------

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | Políticas de acesso do usuário são estabelecidas. |
| <input type="checkbox"/> | <input type="checkbox"/> | Dados sensíveis (PII/SPII) são confidenciais/privados. |
| <input type="checkbox"/> | <input type="checkbox"/> | A integridade dos dados garante que os dados sejam consistentes, completos, precisos e tenham sido validados. |
| <input type="checkbox"/> | <input type="checkbox"/> | 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): Nesta seção, forneça recomendações relacionadas a controles e/ou necessidades de conformidade que seu gerente de TI pode comunicar às partes interessadas para reduzir riscos aos ativos e melhorar a postura de segurança da Botium Toys.