

Lista de verificação de controles e conformidade

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

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	Ao controle
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Ultimo privilégio
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Planos de recuperação de desastres
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Políticas de senha
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separação de deveres
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sistema de detecção de intrusão (IDS)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cópias de segurança
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Software antivírus
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitoramento, manutenção e intervenção manual para sistemas legados
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Criptografia
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sistema de gerenciamento de senha
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Fechaduras (escritórios, vitrine, armazém)

- | | | |
|-------------------------------------|--------------------------|---|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Vigilância em circuito fechado de televisão (CCTV) |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Deteção/prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.) |

Para completar a lista de verificação de conformidade, consulte as informações fornecidas no [escopo, metas e relatório de avaliação de risco](#). Para obter mais detalhes sobre cada regulamento de conformidade, consulte o [controles, estruturas e conformidade](#) leitura.

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

Lista de verificação de conformidade

Padrão de segurança de dados da indústria de cartões de pagamento (PCI DSS)

Sim	Não	Melhor prática
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Somente usuários autorizados têm acesso às informações do cartão de crédito dos clientes.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	As informações do cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Implementar procedimentos de criptografia de dados para proteger melhor os dados e pontos de contato de transações de cartão de crédito.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Adotar políticas seguras de gerenciamento de senhas.

Regulamento Geral de Proteção de Dados (RGPD)

Sim	Não	Melhor prática
<input type="checkbox"/>	<input checked="" type="checkbox"/>	UE. os dados dos clientes são mantidos privados/protegidos.

- | | | |
|-------------------------------------|-------------------------------------|---|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Existe um plano em vigor para notificar a E.U. clientes dentro de 72 horas se seus dados forem comprometidos/houver uma violação. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Certifique-se de que os dados sejam devidamente classificados e inventariados. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Aplica 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 | Melhor prática |
|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Políticas de acesso de usuários são estabelecidas. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Dados confidenciais (PII/SPII) são confidenciais/privados. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | A integridade dos dados garante que os dados sejam consistentes, completos, precisos e validados. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Os dados estão disponíveis para indivíduos autorizados a acessá-los. |

Recomendações: A Botium Toys precisa implementar diversas melhorias na sua segurança, para evitar futuros problemas de vazamento de dados, desastres e acessos não autorizados. Precisa implementar uma política de acesso mais rígida com privilégio mínimo, políticas de senha e a separações de funções para ter o acesso aos dados, além de criptografia.