Checklist para verificar controles e conformidade

Selecione “Sim” ou “não” para responder a pergunta: “A Botium Toys tem esse controle atualmente?”

Lista de verificação de avaliação de controles

Sim	Não	Controle	*Explicação*
☐	☑	Menor privilégio	*Atualmente, todos os funcionários têm acesso aos dados dos clientes; os privilégios precisam ser limitados para reduzir o risco de violação.*
☐	☑	Planos de recuperação de desastres	*Não há planos de recuperação de desastres em vigor. Eles precisam ser implementados para garantir a continuidade dos negócios.*
☐	☑	Políticas de senha	*Os requisitos de senha dos funcionários são mínimos, o que pode permitir que um agente de ameaça acesse mais facilmente dados seguros/outros ativos por meio do equipamento de trabalho dos funcionários/rede interna.*
☐	☑	Separação de funções	*Precisa ser implementado para reduzir a possibilidade de fraude/acesso a dados críticos, já que o CEO da empresa atualmente executa as operações diárias e gerencia a folha de*

			pagamento.
☑	☐	Firewall	*O firewall existente bloqueia o tráfego com base em um conjunto adequadamente definido de regras de segurança.*
☐	☑	Sistema de detecção (IDS)	*O departamento de TI precisa de um IDS para ajudar a identificar possíveis intrusões de agentes de ameaças.*
☐	☑	Backups	*O departamento de TI precisa ter backups de dados críticos, no caso de uma violação, para garantir a continuidade dos negócios.*
☑	☐	Antivirus software	*O software antivírus é instalado e monitorado regularmente pelo departamento de TI.*
☐	☑	Monitoramento manual, manutenção e intervenção para sistemas legados	*A lista de ativos observa o uso de sistemas legados. A avaliação de risco indica que esses sistemas são monitorados e mantidos, mas não há um cronograma regular para essa tarefa e os procedimentos/políticas relacionados à intervenção não são claros, o que pode colocar esses sistemas em risco de violação.*
☐	☑	Criptografia	*A criptografia não é usada atualmente; implementá-la proporciona maior confidencialidade de informações confidenciais.*

☐	☑	Sistema de gerenciamento de senha	*Não há um sistema de gerenciamento de senhas em vigor atualmente; implementar esse controle melhoraria a produtividade do departamento de TI/outros funcionários em caso de problemas de senha.*
☑	☐	Fechaduras (escritórios, armazéns, vitrines)	*A localização física da loja, que inclui os escritórios principais da empresa, a fachada da loja e o depósito de produtos, possui fechaduras suficientes.*
☑	☐	Circuito fechado de televisão CFTV	*O CFTV está instalado/funcionando no local físico da loja.*
☑	☐	Detecção/Prevenção de incêndio	*A localização física da Botium Toys possui um sistema de detecção e prevenção de incêndio em funcionamento.*

Lista de verificação de conformidade

Selecione “sim” ou “não” para responder à pergunta: A Botium Toys atualmente adere a esta melhor prática de conformidade?

Payment Card Industry Data Security Standard (PCI DSS)

Sim	Não	Melhores práticas	*Explicação*
☐	☑	Somente usuários autorizados têm acesso às informações do cartão de crédito dos clientes.	*Atualmente, todos os funcionários têm acesso aos dados internos da empresa.*
☐	☑	As informações do cartão de	*As informações do cartão de*

		crédito são aceitas, processadas, transmitidas e armazenadas internamente, em um ambiente seguro.	*crédito não são criptografadas e todos os funcionários atualmente têm acesso aos dados internos, incluindo as informações do cartão de crédito dos clientes.*
☐	☑	Implemente procedimentos de criptografia de dados para proteger melhor os pontos de contato e os dados das transações de cartão de crédito.	*Atualmente, a empresa não usa criptografia para garantir melhor a confidencialidade das informações financeiras dos clientes.*
☐	☑	Adote políticas seguras de gerenciamento de senhas.	*As políticas de senha são nominais e não há nenhum sistema de gerenciamento de senhas em vigor no momento.*

General Data Protection Regulation (GDPR)

Sim	Não	Melhores práticas	*Explicação*
☐	☑	Os dados dos clientes da U.E. são mantidos privados/seguros.	*Atualmente, a empresa não usa criptografia para garantir melhor a confidencialidade das informações financeiras dos clientes.*
☑	☐	Existe um plano para notificar os clientes da UE dentro de 72 horas se seus dados forem comprometidos/houver uma violação.	*Há um plano para notificar clientes da UE dentro de 72 horas sobre uma violação de dados.*
☐	☑	Garanta que os dados sejam devidamente classificados e inventariados.	*Os ativos circulantes foram inventariados/listados, mas não classificados.*
☑	☐	Aplique políticas, procedimentos e processos de privacidade para documentar e manter dados adequadamente.	*Políticas, procedimentos e processos de privacidade foram desenvolvidos e aplicados entre os membros da equipe de TI e outros funcionários, conforme necessário.*

System and Organizations Controls (SOC type 1, SOC type 2)

Sim	Não	Melhores práticas	*Explicação*
☐	☑	Políticas de acesso do usuário são estabelecidas.	*Controles de privilégio mínimo e separação de funções não estão em vigor atualmente; todos os funcionários têm acesso aos dados armazenados internamente.*
☐	☑	Dados confidenciais (PII/SPII) são confidenciais/privados.	*A criptografia não é usada atualmente para garantir melhor a confidencialidade de PII/SPII.*
☑	☐	A integridade dos dados garante que eles sejam consistentes, completos, precisos e tenham sido validados.	*A integridade dos dados está em vigor.*
☐	☑	Os dados estão disponíveis para indivíduos autorizados a acessá-los.	*Embora os dados estejam disponíveis para todos os funcionários, a autorização precisa ser limitada apenas aos indivíduos que precisam acessá-los para realizar seu trabalho.*

Recomendações: Para melhorar a postura de segurança da Bottum Toys e garantir a conformidade com as melhores práticas de segurança e proteção de dados, as seguintes recomendações são sugeridas:

Implementação do Princípio do Privilégio Mínimo: Limitar o acesso aos dados dos clientes e outras informações sensíveis apenas aos funcionários que necessitam

desses dados para realizar suas funções. Isso reduzirá o risco de violações de dados e acessos não autorizados.

Desenvolvimento de Planos de Recuperação de Desastres: Criar e implementar planos de recuperação de desastres para garantir a continuidade dos negócios em caso de interrupções ou incidentes graves. Isso inclui a definição de procedimentos claros para a restauração de sistemas e dados críticos.

Reforço das Políticas de Senha: Estabelecer políticas de senha mais robustas, incluindo requisitos de complexidade e renovação periódica. Isso ajudará a prevenir acessos não autorizados através de credenciais comprometidas.

Separação de Funções: Implementar a separação de funções para reduzir o risco de fraudes e acessos indevidos a dados críticos. Isso significa que uma única pessoa não deve ter controle total sobre processos sensíveis, como a gestão da folha de pagamento.

Implementação de um Sistema de Detecção de Intrusões (IDS): Adotar um IDS para monitorar a rede e identificar possíveis tentativas de intrusão por agentes de ameaças. Isso ajudará a detectar e responder a incidentes de segurança de forma mais eficiente.

Gerenciamento Contínuo de Sistemas Legados: Estabelecer um cronograma regular para monitoramento, manutenção e intervenção em sistemas legados. Isso inclui a definição de procedimentos claros para garantir que esses sistemas não se tornem pontos fracos na segurança da empresa.

Implementação de Criptografia: Adotar a criptografia para proteger informações confidenciais, tanto em trânsito quanto em repouso. Isso garantirá maior confidencialidade e integridade dos dados sensíveis.

Sistema de Gerenciamento de Senhas: Implementar um sistema de gerenciamento de senhas para melhorar a produtividade do departamento de TI e facilitar a recuperação de senhas em caso de problemas.

Classificação de Ativos: Realizar uma classificação adequada dos ativos da empresa para identificar quais controles adicionais precisam ser implementados. Isso ajudará a priorizar os esforços de segurança e proteger melhor as informações sensíveis.

Conformidade com PCI DSS e GDPR: Implementar controles como criptografia, políticas de gerenciamento de senhas e separação de funções para atender aos requisitos do PCI DSS e GDPR. Além disso, garantir que os dados dos clientes da UE sejam mantidos seguros e que haja um plano claro para notificar os clientes em caso de violação de dados.

Revisão e Atualização de Políticas de Segurança: Revisar e atualizar regularmente as políticas, procedimentos e processos de segurança para garantir que estejam alinhados com as melhores práticas e regulamentações atuais.

Conclusão: A implementação dessas recomendações ajudará a Bottum Toys a reduzir os riscos aos seus ativos, melhorar sua postura de segurança e garantir a conformidade com as regulamentações aplicáveis. É essencial que a empresa adote uma abordagem proativa para a gestão de riscos e a proteção de dados, garantindo a confiança dos clientes e a continuidade dos negócios.