Checklist de controles e compliance

Digite um X na coluna “sim” ou “não” para responder à pergunta: A Botium Toys atualmente possui esse controle?

Lista de verificação de avaliação de controles

Sim	Não	Controle	Explicação
	x	Privilégio mínimo	Atualmente, todos os colaboradores têm acesso aos dados dos clientes; os privilégios precisam ser limitados para reduzir o risco de violação.
	x	Planos de recuperação de desastres	Não há planos de recuperação de desastres em vigor. Eles precisam ser implementados para garantir a continuidade dos negócios.
	x	Política de senhas	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 do funcionário/rede interna.
	x	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 do dia a dia e gerencia a folha de pagamento.
x		Firewall	O firewall existente bloqueia o tráfego com base em um conjunto de regras de segurança adequadamente definido.
	x	Sistema de detecção de intrusão (IDS)	O departamento de TI precisa de um IDS em vigor para ajudar a identificar possíveis intrusões por agentes de ameaça.
	x	Backups	O departamento de TI precisa ter backups de dados críticos, no caso de uma violação, para garantir a continuidade dos negócios.
x	x	Antivirus	O antivírus é instalado e monitorado regularmente pelo departamento de TI.
	x	Monitoramento, manutenção e intervenção manual para sistemas	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

		legados	relacionados à intervenção não são claros, o que pode colocar esses sistemas em risco de violação.
	x	Criptografia	A criptografia não é usada atualmente; implementá-la forneceria maior confidencialidade de informações confidenciais.
	x	Sistema de gerenciamento de senha	Não há um sistema de gerenciamento de senhas atualmente em vigor; implementar esse controle melhoraria a produtividade do departamento de TI/outros funcionários no caso de problemas de senha.
x		Fechaduras (escritórios, montra, armazém)	A localização física da loja, que inclui os escritórios principais da empresa, a fachada da loja e o depósito de produtos, tem fechaduras suficientes.
x		Vigilância em circuito fechado de televisão (CCTV)	O CFTV está instalado/funcionando na localização física da loja.
x		Detecção/prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.)	A localização física da Botium Toys tem um sistema de detecção e prevenção de incêndio em funcionamento.

Lista de verificação de conformidade

Digite um X na coluna “sim” ou “não” para responder à pergunta: A Botium Toys atualmente adere a essas práticas recomendadas de conformidade?

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

Sim	Não	Melhor prática	Explicação
	x	Somente usuários autorizados têm acesso às informações do cartão de crédito dos clientes.	Atualmente, todos os funcionários têm acesso aos dados internos da empresa.
	x	As informações do cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro.	As informações do cartão de crédito não são criptografadas e todos os funcionários atualmente têm acesso aos dados internos, incluindo as informações do cartão de crédito dos clientes.
	x	Implemente procedimentos de criptografia de dados para	A empresa não usa criptografia atualmente para garantir melhor a

		proteger melhor os dados e pontos de contato de transações de cartão de crédito.	confidencialidade das informações financeiras dos clientes.
	x	Adote políticas seguras de gerenciamento de senhas.	As políticas de senha são nominais e nenhum sistema de gerenciamento de senha está em vigor atualmente.

Regulamento Geral de Proteção de Dados (GDPR)

Sim	Não	Melhor prática	Explicação
	x	Os dados dos clientes são mantidos privados/protegidos.	A empresa não usa criptografia atualmente para garantir melhor a confidencialidade das informações financeiras dos clientes.
x		Existe um plano em vigor para notificar a E.U. clientes dentro de 72 horas se seus dados forem comprometidos/houver uma violação.	Há um plano para notificar os clientes da U.E. dentro de 72 horas de uma violação de dados.
	x	Certifique-se de que os dados sejam devidamente classificados e inventariados.	Os ativos atuais foram inventariados/listados, mas não classificados.
x		Aplique políticas, procedimentos e processos de privacidade para documentar e manter os dados adequadamente.	Políticas, procedimentos e processos de privacidade foram desenvolvidos e aplicados entre os membros da equipe de TI e outros funcionários, conforme necessário.

Controles de sistema e organizações (SOC tipo 1, SOC tipo 2)

Sim	Não	Melhor prática	Explicação
	x	Políticas de acesso de usuários são estabelecidas.	Controles de Privilégio Mínimo e separação de tarefas não estão em vigor

			atualmente; todos os funcionários têm acesso a dados armazenados internamente.
	x	Dados confidenciais (PII/SPII) são confidenciais/privados.	A criptografia não é usada atualmente para garantir melhor a confidencialidade de PII/SPII.
x		A integridade dos dados garante que os dados sejam consistentes, completos, precisos e validados.	A integridade dos dados está em vigor.
	x	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 de acesso a eles para fazer seus trabalhos.

Recomendações: Diversos controles devem ser implementados para fortalecer a postura de segurança da Botium Toys e proteger com maior eficácia a confidencialidade das informações sensíveis. Entre os principais controles necessários estão: aplicação do princípio do Privilégio Mínimo, elaboração de planos de recuperação de desastres, implementação de políticas de senha robustas, separação de funções, uso de sistemas de detecção de intrusão (IDS), gerenciamento contínuo de sistemas legados, adoção de criptografia e implantação de um sistema eficaz de gerenciamento de senhas.

Para superar as lacunas de conformidade, a Botium Toys precisa adotar medidas como o princípio do privilégio mínimo, separação de funções e criptografia. Além disso, é essencial classificar adequadamente os ativos da empresa, a fim de identificar controles adicionais que possam ser necessários para fortalecer ainda mais a segurança e proteger informações sensíveis.