Checklist de Controles e Conformidade

# Checklist de Avaliação de Controles

"Sim" ou "não" responde à pergunta relacionada a cada controle listado abaixo.

- Privilégio mínimo [ ] Sim [x] Não

- Planos de recuperação de desastres [ ] Sim [x] Não

- Políticas de senha [x] Sim [ ] Não

- Separação de funções [ ] Sim [x] Não

- Firewall [x] Sim [ ] Não

- Sistema de detecção de intrusão (IDS) [ ] Sim [x] Não

- Backups [ ] Sim [x] Não

- Software antivírus [x] Sim [ ] Não

- Monitoramento, manutenção e intervenção manual em sistemas legados [ ] Sim [x] Não

- Criptografia [ ] Sim [x] Não

- Sistema de gerenciamento de senhas [ ] Sim [x] Não

- Trancas (escritórios, loja, armazém) [x] Sim [ ] Não

- Monitoramento por CFTV (circuito fechado de TV) [x] Sim [ ] Não

- Detecção/prevenção de incêndio (alarme de incêndio, sistema de sprinklers etc.)

[x] Sim [ ] Não

# Checklist de Conformidade

"Sim" ou "não" responde à pergunta abaixo relacionada a cada prática recomendada de conformidade.

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

- Somente usuários autorizados têm acesso às informações de cartão de crédito dos clientes. [ ] Sim [x] Não

- As informações de cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro. [ ] Sim [x] Não

- Procedimentos de criptografia de dados são implementados para proteger melhor os pontos de transação e dados. [ ] Sim [x] Não

- Políticas seguras de gerenciamento de senhas são adotadas. [ ] Sim [x] Não

# Regulamento Geral de Proteção de Dados (GDPR)

- Os dados de clientes da União Europeia são mantidos privados/seguros. [ ] Sim [x] Não

- Existe um plano para notificar os clientes da UE em até 72 horas caso seus dados sejam comprometidos. [x] Sim [ ] Não

- Garantir que os dados estejam devidamente classificados e inventariados. [ ] Sim [x] Não

- Aplicar políticas e procedimentos de privacidade para documentar e manter os dados adequadamente. [x] Sim [ ] Não

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

- As políticas de acesso de usuários estão estabelecidas. [ ] Sim [x] Não

- Dados sensíveis (PII/SPII) são confidenciais/privados. [ ] Sim [x] Não

- A integridade dos dados garante que eles sejam consistentes, completos, precisos e validados. [x] Sim [ ] Não

- Os dados estão disponíveis para indivíduos autorizados a acessá-los. [ ] Sim [x] Não

# Recomendações para o gerente de TI

# **Prioridade Alta (Riscos Críticos e Conformidade)**

1. Implementar política de Privilégio Mínimo

* Criar perfis de acesso com base em funções (RBAC).
* Garantir que os usuários tenham apenas as permissões necessárias para executar suas tarefas.

1. Estabelecer plano de recuperação de desastres (Disaster Recovery Plan)

* Documentar procedimentos para restauração de serviços após incidentes.
* Realizar testes periódicos de recuperação.

1. Implantar sistema de backups regulares

* Automatizar backups de dados críticos.
* Armazenar cópias em local seguro e validar a integridade regularmente.

1. Adotar criptografia de dados sensíveis e de transações (PCI DSS)

* Usar criptografia em repouso e em trânsito para proteger dados de cartão de crédito e PII/SPII.
* Atualizar infraestrutura para suportar algoritmos modernos (ex: AES-256, TLS 1.3).

1. Estabelecer sistema de detecção de intrusão (IDS)

* Implementar solução IDS para monitorar tráfego de rede em tempo real.
* Integrar com firewall e antivírus para resposta automatizada a incidentes.

1. Política segura de gerenciamento de senhas

* Estabelecer complexidade mínima (número de caracteres, letras maiúsculas, números e símbolos).
* Implementar ciclo de renovação e bloqueio após tentativas incorretas.

1. Implantar sistema de gerenciamento de senhas centralizado

* Facilitar a aplicação da política de senhas e reduzir chamadas para reset.
* Utilizar ferramentas como Bitwarden, LastPass for Business etc.

# **Prioridade Média (Boas Práticas de Conformidade e Gestão de Risco)**

1. Implementar política de Separação de Funções (SoD)

* Definir funções críticas que devem ser separadas para evitar fraudes internas e erros acidentais.

1. Inventariar e classificar todos os dados

* Estabelecer uma política de classificação de dados com rótulos como “Público”, “Confidencial”, “Restrito”.
* Integrar essa política a controles de acesso.

1. Estabelecer políticas formais de acesso a dados (SOC 1/2)

* Documentar critérios de concessão de acesso, revisão periódica e revogação.

1. Garantir treinamentos periódicos com os funcionários.

# **Prioridade Baixa (Controles operacionais complementares)**

1. Agendar manutenções regulares dos sistemas legados

* Estabelecer cronograma de verificação e documentação técnica.
* Avaliar roadmap de substituição.

1. Fortalecer a conscientização em segurança

* Realizar treinamentos de segurança da informação com todos os funcionários.
* Simular cenários de phishing e resposta a incidentes.

# **Comunicação com Stakeholders**

A ausência de controles críticos como backups, criptografia, IDS e políticas de acesso representa um alto risco à confidencialidade, integridade e disponibilidade dos ativos da Botium Toys. Recomendamos priorizar a implementação dessas medidas para alcançar conformidade com normas como PCI DSS, GDPR e SOC 2 e proteger os dados de clientes e da empresa contra perdas e violações.