# 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. Implementar política de privacidade abrangente

* Integrar procedimentos GDPR e LGPD.
* 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.