Botium Toys – Auditoria Interna de Segurança Cibernética

Data: 30/06/2025

1. Lista de Verificação de Controles

- Least Privilege: Não
- Disaster recovery plans: Não
- Password policies: Não
- Separation of duties: Não
- Firewall: Sim
- Intrusion detection system (IDS): Não
- Backups: Não
- Antivirus software: Sim
- Manual monitoring, manutenção de sistemas legados: Não
- Encryption: Não
- Password management system: Não
- Locks (escritórios, loja, depósito): Sim
- Closed-circuit television (CCTV) surveillance: Sim
- Fire detection/prevention (alarme de incêndio, sprinklers, etc.): Sim

2. Verificação de Conformidade

PCI DSS

- Apenas usuários autorizados têm acesso a dados de cartão: Não
- Dados de cartão são processados em ambiente seguro: Não
- Procedimentos de criptografia implementados: Não
- Políticas seguras de gerenciamento de senhas: Não

GDPR

- Dados de clientes da UE são mantidos privados/seguros: Sim
- Plano de notificação em até 72h em caso de violação de dados: Sim
- Dados classificados e inventariados corretamente: Não
- Políticas e processos de privacidade são aplicados e documentados: Sim

SOC 1 / SOC 2

- Políticas de acesso de usuários estão estabelecidas: Não
- Dados sensíveis (PII/SPII) são privados: Não
- Integridade dos dados (completos, válidos, precisos): Sim
- Dados disponíveis apenas a pessoas autorizadas: Não

3. Recomendações para o Gerente de TI

1. Implementar controles de acesso com base no princípio do menor privilégio e separação de funções.
2. Estabelecer políticas de senhas robustas e um sistema de gerenciamento centralizado.

3. Adotar soluções de criptografia para proteger dados sensíveis e de cartão de crédito.
4. Implementar backups regulares e um plano de recuperação de desastres.
5. Instalar e configurar um sistema de detecção de intrusos (IDS).
6. Inventariar e classificar todos os ativos da empresa.