# Botium Toys: Escopo, objetivos e relatório de avaliação de risco

## Escopo e objetivos da auditoria

**Escopo:** O escopo é definido como todo o programa de segurança da Botium Toys. Isso significa que todos os ativos precisam ser avaliados juntamente com processos e procedimentos internos relacionados à implementação de controles e melhores práticas de conformidade.

**Objetivos:** Avaliar os ativos existentes e concluir a lista de verificação de controles e conformidade para determinar quais controles e melhores práticas de conformidade precisam ser implementados para melhorar a postura de segurança da Botium Toys.

## Ativos atuais

Os ativos gerenciados pelo Departamento de TI incluem:

* Equipamentos locais para necessidades comerciais no escritório
* Equipamentos para funcionários: dispositivos de usuário final (desktops/laptops, smartphones), estações de trabalho remotas, fones de ouvido, cabos, teclados, mouses, estações de encaixe, câmeras de vigilância, etc.
* Produtos de vitrine disponíveis para venda no varejo no local e online; armazenados no depósito adjacente da empresa
* Gerenciamento de sistemas, software e serviços: contabilidade, telecomunicações, banco de dados, segurança, comércio eletrônico e gerenciamento de estoque
* Acesso à Internet
* Rede interna
* Retenção e armazenamento de dados
* Manutenção de sistema legado: sistemas em fim de vida útil que exigem monitoramento humano

## Risk assessment

### Descrição do risco

Atualmente, há um gerenciamento inadequado de ativos. Além disso, a Botium Toys não tem todos os controles adequados em vigor e pode não estar totalmente em conformidade com os regulamentos e padrões dos EUA e internacionais.

### Melhores práticas de controle

A primeira das cinco funções do NIST CSF é Identificar. A Botium Toys precisará dedicar recursos para identificar ativos para que possam gerenciá-los adequadamente. Além disso, eles precisarão classificar os ativos existentes e determinar o impacto da perda de ativos existentes, incluindo sistemas, na continuidade dos negócios.

### Pontuação de risco

Em uma escala de 1 a 10, a pontuação de risco é 8, o que é bastante alto. Isso se deve à falta de controles e adesão às melhores práticas de conformidade.

### Comentários adicionais

O impacto potencial da perda de um ativo é classificado como médio, porque o departamento de TI não sabe quais ativos estariam em risco. O risco de ativos ou multas de órgãos governamentais é alto porque a Botium Toys não tem todos os controles necessários em vigor e não está aderindo totalmente às melhores práticas relacionadas aos regulamentos de conformidade que mantêm dados críticos privados/seguros. Revise os seguintes pontos para obter detalhes específicos:

* Atualmente, todos os funcionários da Botium Toys têm acesso a dados armazenados internamente e podem acessar dados do titular do cartão e PII/SPII dos clientes.
* A criptografia não é usada atualmente para garantir a confidencialidade das informações do cartão de crédito dos clientes que são aceitas, processadas, transmitidas e armazenadas localmente no banco de dados interno da empresa.
* Os controles de acesso relativos ao menor privilégio e à separação de funções não foram implementados.
* O departamento de TI garantiu a disponibilidade e os controles integrados para garantir a integridade dos dados.
* O departamento de TI tem um firewall que bloqueia o tráfego com base em um conjunto de regras de segurança adequadamente definido.
* O software antivírus é instalado e monitorado regularmente pelo departamento de TI.
* O departamento de TI não instalou um sistema de detecção de intrusão (IDS).
* Não há planos de recuperação de desastres em vigor atualmente, e a empresa não tem backups de dados críticos.
* O departamento de TI estabeleceu um plano para notificar os clientes da U.E. dentro de 72 horas se houver uma violação de segurança. Além disso, políticas, procedimentos e processos de privacidade foram desenvolvidos e são aplicados entre os membros do departamento de TI/outros funcionários, para documentar e manter os dados adequadamente.
* Embora exista uma política de senha, seus requisitos são nominais e não estão de acordo com os requisitos mínimos atuais de complexidade de senha (por exemplo, pelo menos oito caracteres, uma combinação de letras e pelo menos um número; caracteres especiais).
* Não há um sistema centralizado de gerenciamento de senhas que aplique os requisitos mínimos da política de senhas, o que às vezes afeta a produtividade quando funcionários/fornecedores enviam um tíquete ao departamento de TI para recuperar ou redefinir uma senha.
* Embora os sistemas legados sejam monitorados e mantidos, não há um cronograma regular para essas tarefas e os métodos de intervenção não são claros.
* A localização física da loja, que inclui os escritórios principais da Botium Toys, a fachada da loja e o depósito de produtos, possui fechaduras suficientes, vigilância de circuito fechado de televisão (CFTV) atualizada, bem como sistemas de detecção e prevenção de incêndio em funcionamento.