Controls and compliance checklist

Auditoria de segurança feita na empresa:

Escopos e metas da auditoria:

Escopo: O escopo desta auditoria é definido como todo o programa de segurança da Botium Toys. Isso inclui seus ativos, como equipamentos e dispositivos dos funcionários, sua rede interna e seus sistemas. Será necessário revisar os ativos que a Botium Toys possui, bem como os controles e práticas de conformidade que estão em vigor.

Objetivos: Avaliar os ativos existentes e preencher 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 circulares:

Ativos gerenciados pelo Departamento de TI incluem:

● Equipamentos locais para as necessidades comerciais no escritório

● Equipamentos dos funcionários: dispositivos de uso final (desktops/notebooks, smartphones), estações de trabalho remotas, headsets, cabos, teclados, mouses, estações de acoplamento (docking stations), câmeras de vigilância etc.

● Produtos disponíveis para venda no ponto de venda físico e online; armazenados no depósito anexo da empresa

● Gerenciamento de sistemas, softwares e serviços: contabilidade, telecomunicações, banco de dados, segurança, comércio eletrônico e gerenciamento de inventário

● Acesso à internet

● Rede interna

● Retenção e armazenamento de dados

● Manutenção de sistemas legados: sistemas obsoletos que exigem monitoramento humano

Risk Assessment (Avaliação de riscos)

Descrição do risco

Atualmente, há uma gestão inadequada dos ativos. Além disso, a Botium Toys não possui todos os controles apropriados implementados e pode não estar em total conformidade com as regulamentações e normas 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 seus ativos, a fim de gerenciá-los adequadamente. Além disso, será necessário classificar os ativos existentes e determinar o impacto da perda desses ativos, 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 relativamente alto. Isso se deve à falta de controles e à não adesão às melhores práticas de conformidade.

Comentários adicionais

O impacto potencial da perda de um ativo é classificado como **médio**, pois o departamento de TI não sabe exatamente quais ativos estariam em risco. O risco relacionado aos ativos ou multas por órgãos reguladores é **alto**, já que a Botium Toys não possui todos os controles necessários implementados e não está seguindo totalmente as melhores práticas relacionadas às normas de conformidade que protegem dados críticos. Veja abaixo os detalhes específicos:

- Atualmente, **todos os funcionários da Botium Toys têm acesso aos dados armazenados internamente** e podem conseguir acessar **dados de cartões de crédito e informações pessoais (PII/SPII)** de clientes.
- **Não há criptografia** utilizada para garantir a confidencialidade das informações dos cartões de crédito dos clientes que são aceitas, processadas, transmitidas e armazenadas localmente no banco de dados interno da empresa.
- **Controles de acesso** relacionados ao **princípio do menor privilégio** e à **separação de funções** não foram implementados.

- O departamento de TI garantiu a **disponibilidade** e implementou **controles para assegurar a integridade dos dados**.
- O departamento de TI possui um **firewall** que bloqueia o tráfego com base em um conjunto de regras de segurança devidamente definidas.
- **Softwares antivírus estão instalados e são monitorados regularmente** pelo departamento de TI.
- O departamento de TI **não instalou um sistema de detecção de intrusão (IDS)**.
- **Não existem planos de recuperação de desastres**, e a empresa **não possui backups de dados críticos**.
- O departamento de TI estabeleceu um plano para **notificar clientes da União Europeia em até 72 horas** em caso de violação de segurança. Além disso, **políticas, procedimentos e processos de privacidade foram desenvolvidos e são aplicados entre os membros do departamento de TI e outros funcionários**, para documentar e manter os dados corretamente.
- Embora exista uma **política de senhas**, seus requisitos são mínimos e **não estão alinhados com os padrões atuais de complexidade mínima** (por exemplo, pelo menos oito caracteres, combinação de letras e ao menos um número; caracteres especiais).
- **Não há um sistema centralizado de gerenciamento de senhas** que imponha os requisitos mínimos da política de senhas, o que às vezes afeta a produtividade quando funcionários ou fornecedores precisam abrir chamados no departamento de TI para recuperar ou redefinir senhas.
- Embora **sistemas legados sejam monitorados e mantidos**, **não existe uma programação regular para essas tarefas** e os métodos de intervenção são incertos.
- A **localização física da loja**, que inclui os **escritórios principais da Botium Toys, loja e depósito de produtos**, possui **trancas adequadas, sistema de vigilância (CCTV) atualizado, além de sistemas funcionais de detecção e prevenção de incêndios**.

Auditoria feita por mim, com recomendações(muito básico):

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place? A botium Toys atualmente possui esse controle em vigor?*

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☐	☑	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☑	☐	Locks (offices, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice? A botium Toys atualmente adere a essas melhores praticas ?*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
☐	☑	Only authorized users have access to customers' credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☑	☐	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☑	☐	E.U. customers' data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classified and inventoried.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☐	☑	Data is available to individuals authorized to access it.

Recommendations:

Como muito mencionado, aqui vai algumas recomendações para o gerente de TI:

- Separação de acessos por funções;
- Acessos menor(apenas acessos necessarios aquela função)
- Politica de senhas, com pelo menos 1 caracter especial, 4 letras, 4 numeros, letra maiuscula, e sem repetição de algo da senha anterior.
- Adicionar planos de recuperação de desastres juntamente trazendo o plano de backups de máquinas de gerentes, servidores e firewall, diariamente.
- Criar um processo que faça isso automaticamente por comandos.
- Monitoramento de sistemas legados mais fortes, ou refatoramento total do sistema legado, para que consiga adicionar novas politicas de segurança nele.
- Instalar sistemas de detecção de instrução nos firewalls e computadores das pessoas que iram fazer o monitoramento
- Adicionar criptografia aos dados bancarios de cada cliente, sendo cartões em geral, criptografia de ponta para que esses dados não sejam acessados por algum agente malicioso externo.