Lista de verificação de controles e conformidade

Lista de verificação com base no escopo, objetivos e relatório de avaliação de riscos da Botium Toys: Escopo, objetivos e relatório de avaliação de riscos.

**Lista de verificação de avaliação de controles**

|  |  |  |
| --- | --- | --- |
| **SIM** | **NÃO** | **CONTROLE** |
|  | X | Menos privilegiado |
|  | X | Plano de recuperção de desastre |
| X |  | Políticas de senhas |
|  | X | Separação de funções |
| X |  | Firewall |
|  | X | Sistema de detecção de intrusos(IDS) |
|  | X | Backups |
| X |  | Software de Antivirus |
| X |  | Monitoramento manual, manutenção e intervenção para sistemas legados |
|  | X | Criptografia |
|  | X | Sistema de Gerenciamento de Senhas |
| X |  | Fechaduras (escritórios, frente da loja, depósito) |
| X |  | Vigilância por circuito fechado de televisão (CCTV) |
| X |  | Detecção/prevenção de incêndios (alarme de incêndio, sistema de sprinklers, etc.) |

**Lista de verificação de conformidade**

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |
| --- | --- | --- |
| **SIM** | **NÃO** | **BOAS PRÁTICAS** |
|  | X | Apenas usuários autorizados têm acesso às informações dos cartões de crédito dos clientes.. |
|  | X | As informações de cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro. |
|  | X | Implemente procedimentos de criptografia de dados para melhorar a segurança nos pontos de contato e dados de transações com cartões de crédito. |
|  | X | Adote políticas seguras de gerenciamento de senhas. |

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **SIM** | **NÃO** | **BOAS PRÁTICAS** |
|  | X | Os dados dos clientes da União Europeia são mantidos privados/seguros. |
| X |  | Os dados dos clientes da União Europeia são mantidos privados/seguros. |
|  | X | Certifique-se de que os dados sejam devidamente classificados e inventariados. |
| X |  | Implemente políticas, procedimentos e processos de privacidade para documentar e manter adequadamente os dados. |

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

|  |  |  |
| --- | --- | --- |
| **SIM** | **NÁO** | **BOAS PRÁTICAS** |
|  | X | Políticas de acesso de usuários são estabelecidas. |
|  | X | Os dados sensíveis (PII/SPII) são confidenciais/privados. |
| X |  | A integridade dos dados garante que os dados sejam consistentes, completos, precisos e tenham sido validados. |
| X |  | Os dados estão disponíveis apenas para indivíduos autorizados a acessá-los. |

**Recomendações :**

Para abordar algumas questões de segurança na postura de segurança da Botium Toys, recomendamos o seguinte:

* Implemente políticas e controles de acesso do usuário para o Gerenciamento de Acesso: Gerenciamento de Acesso Baseado em Funções, Gerenciamento de Acesso Obrigatório ou Gerenciamento de Acesso Discricionário. Isso garantirá que apenas pessoas autorizadas possam acessar dados sensíveis..
* Criptografia de dados em todos os estados: em repouso, em uso ou em movimento..
* Aplicação dos princípios de separação de funções e menos privilégiado.
* Estabelecer um Plano de Continuidade de Negócios (BCP) e um Plano de Recuperação de Desastres (DRP), com backups como parte do DRP.
* Reforce as políticas de senhas com requisitos mais complexos e implemente um sistema centralizado de gerenciamento de senhas para melhorar a produtividade quando funcionários/fornecedores enviarem uma solicitação ao departamento de TI para recuperar ou redefinir uma senha.
* Implemente um Firewall de Próxima Geração com IDS integrado.
* Utilize um ambiente seguro para garantir que as informações do cartão de crédito sejam armazenadas, aceitas, processadas e transmitidas internamente de maneira segura.
* Realize periodicamente um Inventário de Ativos, categorizando e rotulando os ativos no processo.