Lista de Verificação de Controles e Conformidade

Para preencher a lista de verificação de avaliação de controles, consulte as informações fornecidas no relatório de escopo, metas e avaliação de risco. Para mais detalhes sobre cada controle, incluindo o tipo e finalidade, consulte o documento de categorias de controles.  
  
Em seguida, selecione “sim” ou “não” para responder à pergunta: A Botium Toys atualmente possui este controle implementado?

# Lista de Verificação de Controles

|  |  |  |
| --- | --- | --- |
| Sim | Não | Controle |
|  | ✔️ | Privilégio mínimo |
|  | ✔️ | Planos de recuperação de desastres |
|  | ✔️ | Políticas de senhas |
|  | ✔️ | Separação de funções |
| ✔️ |  | Firewall |
|  | ✔️ | Sistema de detecção de intrusões (IDS) |
|  | ✔️ | Backups |
| ✔️ |  | Software antivírus |
| ✔️ |  | Monitoramento, manutenção e intervenção manual para sistemas legados |
|  | ✔️ | Criptografia |
|  | ✔️ | Sistema de gerenciamento de senhas |
| ✔️ |  | Trancas (escritórios, loja, armazém) |
| ✔️ |  | Vigilância por circuito fechado de TV (CCTV) |
| ✔️ |  | Detecção/prevenção de incêndio (alarme de incêndio, sprinklers, etc.) |

# Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento (PCI DSS)

|  |  |  |
| --- | --- | --- |
| Sim | Não | Prática recomendada |
|  | ✔️ | Somente usuários autorizados têm acesso às informações de cartão de crédito dos clientes. |
|  | ✔️ | As informações de cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente em um ambiente seguro. |
|  | ✔️ | Implementar procedimentos de criptografia de dados para proteger pontos de transação e dados de cartões de crédito. |
|  | ✔️ | Adotar políticas seguras de gerenciamento de senhas. |

# Regulamento Geral de Proteção de Dados (GDPR)

|  |  |  |
| --- | --- | --- |
| Sim | Não | Prática recomendada |
|  | ✔️ | Os dados dos clientes da UE são mantidos privados/seguros. |
| ✔️ |  | Existe um plano para notificar os clientes da UE em até 72 horas caso seus dados sejam comprometidos/haja uma violação. |
|  | ✔️ | Garantir que os dados sejam devidamente classificados e inventariados. |
| ✔️ |  | Aplicar políticas, procedimentos e processos de privacidade para documentar e manter os dados de forma adequada. |

# Controles de Sistemas e Organizações (SOC tipo 1, SOC tipo 2)

|  |  |  |
| --- | --- | --- |
| Sim | Não | Prática recomendada |
|  | ✔️ | Políticas de acesso de usuários estão estabelecidas. |
|  | ✔️ | Dados sensíveis (PII/SPII) são mantidos confidenciais/privados. |
| ✔️ |  | A integridade dos dados garante que eles sejam consistentes, completos, precisos e validados. |
|  | ✔️ | Os dados estão disponíveis para indivíduos autorizados a acessá-los. |

# Recomendações (opcional)

Diversos controles precisam ser implementados para melhorar a postura de segurança da Botium Toys e garantir melhor confidencialidade das informações sensíveis, incluindo: Privilégio Mínimo, planos de recuperação de desastres, políticas de senhas, separação de funções, um IDS, gerenciamento contínuo de sistemas legados, criptografia e um sistema de gerenciamento de senhas.  
  
Para resolver as lacunas de conformidade, a Botium Toys precisa implementar controles como Privilégio Mínimo, separação de funções e criptografia. A empresa também precisa classificar adequadamente os ativos para identificar controles adicionais necessários à proteção das informações sensíveis.