**Controles e lista de verificação de conformidade**

*Para concluir a lista de verificação de avaliação de controles, consulte as informações fornecidas no relatório de avaliação de escopo, metas e risco. Para obter mais detalhes sobre cada controle, incluindo o tipo e a finalidade, consulte o documento de categorias de controle.*

*Em seguida, digite na coluna "sim" ou "não" para responder à pergunta: A Botium Toys tem atualmente esse controle?*

**Lista de verificação de avaliação de controles**

|  |  |
| --- | --- |
| **Atende** | **Controle** |
| Não | Privilégio mínimo |
| Não | Planos de recuperação de desastre |
| Não | Políticas de senha |
| Não | Separação de funções |
| Sim | Firewall |
| Não | Sistema de detecção de intrusão (IDS) |
| Não | Backups |
| Sim | Software antivírus |
| Não | Monitoramento, manutenção e intervenção manuais para sistemas legado |
| Não | Encriptação |
| Não | Sistema de gerenciamento de senhas |
| Sim | Fechaduras (escritórios, vitrine, armazém) |
| Sim | Circuito fechado de televisão (CCTV) de vigilância |
| Sim | Detecção/prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.) |

*Para concluir a lista de verificação de conformidade, consulte as informações fornecidas no relatório de avaliação de escopo, metas e risco. Para obter mais detalhes sobre cada regulamento de conformidade, revise os controles, as estruturas e a leitura de conformidade.*

*Em seguida, digite na coluna "sim" ou "não" para responder à pergunta: A Botium Toys atualmente adere a essa prática recomendada de conformidade?*

**Lista de verificação de conformidade**

Padrão de segurança de dados da indústria de cartões de pagamento (PCI DSS)

|  |  |
| --- | --- |
| **Atende** | **Melhores práticas** |
| Não | Somente usuários autorizados tem acesso às informações de cartão de crédito dos clientes |
| Não | As informações de cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro |
| Não | Implementação de procedimentos de criptografia de dados para proteger melhor os pontos de contato e os dados de transações de cartão de crédito |
| Não | Adoção de políticas seguras de gerenciamento de senhas |

Regulamento Geral sobre a Proteção de Dados (GRPD)

|  |  |
| --- | --- |
| **Atende** | **Melhores práticas** |
| Sim | Os dados dos clientes da UE são mantidos privados/protegidos. |
| Sim | Existe um plano em vigor para notificar os clientes da UE dentro de 72 horas se seus dados forem comprometidos/houver uma violação. |
| Não | Certificação de que os dados são devidamente classificados e inventariados. |
| Não | Aplicação de políticas, procedimentos e processos de privacidade para documentar e manter dados adequadamente. |

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

|  |  |
| --- | --- |
| **Atende** | **Melhores práticas** |
| Não | As políticas de acesso do usuário são estabelecidas. |
| Não | Os dados confidenciais (PII/SPII) são confidenciais/privados. |
| Sim | A integridade dos dados garante que os dados sejam consistentes, completos, precisos e validados. |
| Não | Os dados estão disponíveis para indivíduos autorizados a acessá-los. |

*Esta seção é opcional e pode ser usada para fornecer um resumo das recomendações ao gerente de TI sobre quais controles e/ou práticas recomendadas de conformidade a Botium Toys precisa implementar, com base no risco representado se não for implementado em tempo hábil.*

**Recomendações (opcional):**

Os dados dos clientes da Botium Toys não estão recebendo o tratamento adequado e estão severamente expostos à vazamentos por atacantes internos ou externos.

Por haver diversas falhas de segurança, não há conformidade com as leis vigentes, e no eminente caso de um vazamento dos dados armazenados pela empresa, são múltiplos os impactos negativos decorrentes destas falhas:

* danos à reputação e imagem da empresa bem como perda de confiança
* impactos financeiros devido a interrupção de continuidade de negócios, custos para correção do erro, perda de clientes
* multas e sanções aplicadas governamentalmente
* processos movidos por clientes em caso de vazamento de dados PII e SPII que podem ocasionar roubo de identidade e fraude destes

Prevenção contra ameaças internas

Adotar o controle de privilégio mínimo e separação de funções aos funcionários da Botium Toys são medidas que mitigam possível comprometimento por ações internas, pois limitam o acesso dos dados apenas a quem realmente precisa.

Prevenção contra ameaças externas

Apesar de dispor de firewall e software antivírus mantidos e monitorados pelo departamento de TI, a Botium Toys está exposta à atacantes externos que disponham de maior nível de conhecimento, tendo em vista a falta de mais mecanismos de defesa. Medidas recomendadas afim de sanar estas vulnerabilidades são:

* criptografia adotada aos dados armazenados dos clientes e possíveis dados de segredo industrial da empresa
* implementação de um sistema de detecção de intrusão (IDS)
* maior rigor nas regras de criação de senhas para funcionários, exigindo mínimo de 8 caracteres, sendo ao menos um em caixa alta, um em caixa baixa, um numeral e um caractere especial, e a adoção da validação multifatorial
* definir e aplicar um cronograma fixo para monitoramento dos sistemas legados até sua substituição total, o que é altamente recomendado e deve ser feito o quanto antes
* criação de um backup de dados, ainda que disponha de mecanismos de defesa contra incêndio e intrusão, defeitos no hardware são imprevisíveis e podem ocorrer sem aviso prévio, um backup armazenado em nuvem, em um servidor confiável, garante que os dados possam ser recuperados, seja por perda de hardware, ransomware ou qualquer vírus que possa comprometer sua disponibilidade.