TOPCERTIFIER
www.topcertifier.com

METODOLOGIA DE ATENDIMENTO PCI-DSS

Padrão de segurança de dados da indústria de cartões de pagamento.

INTRODUÇÃO PCI DSS

TOPCertifier apresenta uma lista de verificação simplificada de análise de lacunas do PCI DSS para ajudá-lo a identificar áreas onde sua organização pode precisar de melhorias para estar em conformidade com PCI DSS (Payment Requisitos do padrão de segurança de dados da indústria de cartões). Esta lista de verificação oferece uma base estrutura para avaliar seu alinhamento com o PCI DSS e serve como uma etapa inicial na avaliando sua conformidade.

SEÇÃO 1: SEGURANÇA DE DADOS

- os dados do cartão de pagamento estão devidamente criptografados durante a transmissão e armazenamento
- Os dados de autenticação confidenciais, como números CVV, não são armazenados após autorização
- existe uma política para proteger os dados do titular do cartão e dados de autenticação confidenciais

SEÇÃO 2: SEGURANÇA DE REDE E FIREWALL

- As configurações de rede e regras de firewall são revisadas e atualizadas regularmente
- existe um diagrama de rede ilustrando o fluxo de dados do titular do cartão
- Existem políticas e procedimentos de segurança para proteger a infraestrutura de rede

SEÇÃO 3: CONTROLE DE ACESSO

- Os privilégios de acesso do usuário são restritos com base na necessidade de conhecimento da empresa?
- a autenticação multifator está implementada para acesso remoto à rede
- As contas de usuário são prontamente desativadas após rescisão ou mudanças de função?

SEÇÃO 4: GESTÃO DE VULNERABILIDADES

- Os patches de segurança são aplicados prontamente para resolver vulnerabilidades?
- existe um processo para verificação de vulnerabilidades e testes de penetração
- Os patches de segurança críticos são revisados e priorizados com base no risco

SEÇÃO 5: POLÍTICAS E PROCEDIMENTOS DE SEGURANÇA

- As políticas e procedimentos de segurança abrangentes são documentados e divulgados
- existe um programa de treinamento de conscientização de segurança para funcionários
- As políticas de segurança são revisadas e atualizadas conforme necessário

SEÇÃO 6: MONITORAMENTO E REGISTRO

- Os eventos e registros de segurança são revisados e monitorados regularmente
- existe um processo para conduzir alertas em tempo real para atividades suspeitas
- Os procedimentos de resposta e notificação de incidentes estão estabelecidos

SEÇÃO 7: RESPOSTA A INCIDENTES

- existe um plano de resposta a incidentes descrevendo etapas para lidar com incidentes de segurança
- Os funcionários são treinados sobre como reconhecer e relatar incidentes de segurança
- existe um processo documentado para análise e melhoria pós-incidente

SEÇÃO 8: SEGURANÇA FÍSICA

- Existem controles de acesso físico para evitar acesso não autorizado aos dados do titular do cartão
- o acesso a áreas seguras é restrito e monitorado
- A vigilância por vídeo e os registros de visitantes são mantidos em áreas sensíveis

SEÇÃO 9: PRESTADORES DE SERVIÇOS TERCEIROS

- Os fornecedores terceirizados são avaliados quanto à conformidade com o PCI DSS?
- Existem acordos escritos com prestadores de serviços para garantir a proteção dos dados do titular do cartão
- Existe um processo para monitorar e avaliar práticas de segurança de terceiros

Observe que esta lista de verificação fornece uma visão geral de alto nível e é essencial realizar uma análise completa específica dos processos e contexto da sua organização. Além disso, é recomendado envolver-se com especialistas ou consultores do PCI DSS para conduzir uma avaliação abrangente análise de lacunas para sua organização.