# UTILIZANDO A ANÁLISE DE MODO E EFEITOS DE FALHA POTENCIAL (FMEA) PARA ATINGIR A CONFORMIDADE COM O PADRÃO DE SEGURANÇA DOS DADOS DO SETOR DE CARTÕES DE PAGAMENTO (PCI DSS)

**Marcus Vicente Mazzillo (FCAV )**
marcus.mazzillo@gmail.com
**Andre Leme Fleury (USP )**
alfleury@usp.br

*Com o avanço na utilização de diferentes tipos de cartões magnéticos para pagamento de transações financeiras, a preocupação com a segurança das informações armazenadas, transmitidas e processadas torna-se foco prioritário para as empresas que fazem parte deste negócio. Visando garantir a segurança dos dados desses cartões, algumas das principais operadoras compartilharam experiências e criaram um conjunto de políticas e procedimentos denominado Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI). Considerando a crescente incidência de fraudes e ataques que ameaçam a continuidade e imagem das empresas que atuam nesta cadeia de valor, este trabalho apresenta uma proposta para fortalecer o processo de obtenção de conformidade com a certificação utilizando a ferramenta de Análise de Modo e Efeito das Falhas (FMEA). Partindo da revisão bibliográfica sobre o tema, a solução proposta apresenta uma forma de utilização do FMEA enquanto ferramenta para obtenção da certificação PCI DSS. Os resultados desta solução são apresentados mostrando a utilização de uma ferramenta utilizada por empresas do ramo automotivo na área de segurança da informação.*

*Palavras-chaves: PCI-DSS, FMEA, Segurança da Informação*

## 1. Introdução

Buscar a certificação de Padrão de Segurança de Dados (*Data Security Standard - DSS*) do Setor de Cartões de Pagamento (*Payment Card Industry - PCI*) tornou–se foco para as empresas que atuam no setor de pagamentos, já que esta tornou-se exigida pelas principais bandeiras de cartão de pagamentos. A obtenção desta certificação envolve diferentes áreas de uma empresa e requer mudanças em seus processos e, eventualmente, na sua cultura. Em muitos casos, para adequar sua estrutura, a organização contrata uma empresa especializada em soluções para Governança, Riscos e Compliance (GRC), que irá realizar uma análise de lacunas buscando identificar em que pontos a empresa candidata a certificação está falhando. O resultado desta análise é um plano de ação, onde são listadas as falhas da empresa em relação aos requisitos que a certificação exige, ficando a cargo da empresa o planejamento e execução das tarefas para que esta consiga obter o certificado.

Esta utilização de análise de lacunas é correta e, se bem conduzida, oferece para a empresa um bom diagnóstico da sua situação atual e de qual será o esforço necessário para obtenção da certificação. A utilização do plano de ação torna–se uma boa forma para conduzir as iniciativas que necessitam intervenção, auxilia na distribuição das tarefas entre as pessoas responsáveis pela solução dos problemas apresentados e viabiliza o acompanhamento do status geral do projeto através das datas de conclusão estipuladas.

Todavia, esta abordagem nem sempre é eficiente, já quem em diversos casos o plano de ação torna–se uma simples lista de tarefas e, dependendo da urgência do projeto, suas datas são estipuladas baseando–se na data de entrega e sem levar em consideração os esforços necessários para cumprir uma determinada tarefa. Isso faz com que o projeto corra o risco de não ser entregue na data acordada, ter os custos maiores que os estipulados e no pior dos casos, falhar na busca pela certificação. Outro ponto é que este plano de ação serve apenas num único momento, pois a certificação é renovada anualmente e o método de análise de lacunas e o plano de ação não fornecem uma forma de monitoramento contínuo da aderência aos requisitos da certificação.

O objetivo desde trabalho é propor uma forma de estruturar o processo de preparação de uma empresa deste setor para a obtenção da certificação utilizando a ferramenta de Análise dos Modos e Efeitos das Falhas (FMEA), capaz de orientar a melhoria continuada dos processos e das soluções instituídas, visando a aderência da empresa em relação aos requisitos da certificação. Não foram identificadas na literatura iniciativas com escopo similar, o que garante a originalidade do estudo e a sua relevância para as organizações que desejarem aplicar os seus resultados. A utilização do FMEA como ferramenta de apoio para a certificação agregou e documentou o conhecimento necessário, formando uma base de conhecimento robusta, que pode ser utilizada em outros projetos, além de incentivar e proporcionar uma forma de garantir a melhoria continua dos projetos e processos da empresa.

Este trabalho está estruturado em quatro seções. A primeira seção faz uma breve introdução dos assuntos abordados no trabalho e apresenta o problema, os objetivos e a relevância do tema da pesquisa. A segunda seção apresenta a literatura pesquisada, que embasou teoricamente o trabalho. A terceira seção apresenta a solução proposta para o problema apresentado. Finalmente, na quarta seção são apresentados os resultados da aplicação da solução proposta.

## 2. Revisão da Literatura

*- Análise de Modo e Efeitos das Falhas (FMEA)*

Segundo o Manual de Referência da Análise de Modo e Efeitos das Falhas (IQA, 2008), FMEA é uma metodologia analítica utilizada para assegurar que os problemas potenciais tenham sido considerados e abordados ao longo de todo processo de desenvolvimento de produtos e processos. É considerado um método para identificar a gravidade dos potenciais efeitos de uma falha e para fornecer uma entrada para as medidas minimizadoras destinadas a reduzir o risco. O FMEA também é definido como uma técnica de engenharia usada para definir, identificar e eliminar falhas conhecidas e/ou potenciais, problemas e erros de um sistema, projeto, processo e/ou serviço, antes que chegue ao consumidor (OMDAHL 1988; ASQC 1983).

Sendo uma atividade multidisciplinar e que afeta todo o processo de realização do produto, a implantação do FMEA tem de ser bem planejada para ser totalmente eficaz, possuir na equipe membros com conhecimentos especializados relevantes, tempo disponível e autoridade ratificada pelo gerenciamento. Em última instância, a direção tem a responsabilidade e a autoridade para o desenvolvimento e manutenção de FMEAs (IQA, 2008)

*- Momento de Implantação do FMEA*

Em toda literatura pesquisada é dada ênfase para o momento em que o FMEA deve ser aplicado. Conforme Stamatis (2003), por definição o FMEA é uma metodologia para maximizar a satisfação do cliente, eliminando e/ou reduzindo problemas conhecidos ou potenciais. Para isso o FMEA deve começar o mais cedo possível mesmo que os todos os fatos e informações ainda não são totalmente conhecidos. Especificamente um programa FMEA deveria começar (STAMATIS, 2003):

- Quando novos sistemas, projetos, produtos, processos ou serviços são projetados;
- Quando sistemas, projetos, processos ou serviços existentes irão mudar sem razão aparente;
- Quando novas aplicações são encontradas para condições existentes de sistemas, projetos, produtos, processos ou serviços;
- Quando melhorias são consideradas para sistemas, projetos, produtos, processos ou serviços existentes.

O Manual de Referência da Análise de Modo e Efeitos das Falhas (IQA, 2008) afirma que o FMEA é concebido para ser uma ação "antes-do-evento" e não um exercício "após-o-fato". Assim, o FMEA dever ser feito antes da implantação de um produto ou processo no qual exista o potencial de falha.

Depois de seu início, o FMEA deve ser considerado um documento vivo e deve refletir sempre o último nível e as últimas ações tomadas, incluindo aquelas que ocorrem após o início da produção (IQA, 2008). Desta forma, nota – se que o FMEA é de fato uma

ferramenta dinâmica de aperfeiçoamento, pois após seu começo, as informações contidas nele serão utilizadas para melhoria continuada do sistema, projeto, processo, produto ou serviço, pois será continuamente atualizado sempre que for necessário (STAMATIS, 2003).

*- Tipos de FMEA*

Segundo o Manual de Referência de Análise de Modo e Efeitos de Falha Potencial (IQA, 2008), o FMEA é divido em dois tipos: Análise de Modo e Efeitos de Falha de Projeto (DFMEA) e a Análise de Modo e Efeitos de Falha de Processo (PFMEA).

O FMEA de Projeto (DFMEA) é definido como uma análise / metodologia disciplinada de identificar modos de falha conhecidos ou potenciais e prover ações de acompanhamento e corretivas antes do produto iniciar seu processo de fabricação (STAMATIS, 2003).

Um DFMEA deve iniciar com o desenvolvimento de informações para compreender o sistema, subsistema, ou componente sendo analisado, e definir seus requisitos e características funcionais (IQA, 2008). O DFMEA é um documento vivo e deve ser iniciado antes da finalização do conceito do projeto, ser atualizado à medida que ocorram alterações ou informações adicionais sejam obtidas ao longo das fases de desenvolvimento do produto, ser fundamentalmente concluído antes de ser liberado o projeto de produção e ser uma fonte de lições aprendidas para futuras iterações de projeto.

O artefato de um DFMEA é um projeto preliminar (que pode ser modificado devido uma informação nova ou modificada) com uma configuração base e especificações funcionais que traduzem os requisitos estabelecidos em processos qualitativos e quantitativos detalhados e características de montagem e serviço (STAMATIS, 2003).

Por sua vez, o objetivo de um FMEA de Processo (PFMEA) é definir, demonstrar e maximizar as soluções de engenharia em resposta a qualidade, confiança, manutenção, custo e produtividade conforme definidos pelo DFMEA e pelo consumidor (STAMATIS, 2003). O PFMEA assume que o produto, como foi projetado, atenderá ao objetivo do projeto. Modos de falha potencial que possam ocorrer devido a uma fraqueza de projeto podem ser incluídos em um PFMEA. Seu efeito e prevenção são cobertos pelo FMEA de Projeto (IQA, 2008).

Como todo documento FMEA o PFMEA é vivo e deve ser iniciado antes ou durante o estágio de viabilidade, ser iniciado antes da preparação do ferramental para produção, levar em consideração todas as operações de fabricação, dos componentes individuais aos conjuntos montados e incluir todos os processos, dentro da planta, que possam impactar as operações de fabricação e montagem, tais como embarque (expedição), recebimento, transporte de material, armazenagem, transportadores ou etiquetagem.

*- Padrão de Segurança de Dados do Setor de cartões de pagamento (PCI-DSS)*

O Padrão de Segurança de Dados (DSS) do Setor de cartões de pagamento (PCI) foi desenvolvido para incentivar e aprimorar a segurança dos dados do titular do cartão e facilitar a ampla adoção de medidas de segurança de dados consistentes no mundo todo. O PCI DSS oferece a base de requisitos técnicos e operacionais projetados para proteger os dados do

titular do cartão. O PCI DSS se aplica a todas as entidades envolvidas no processo de pagamento do cartão – inclusive comerciantes, financeiras, adquirentes, emissores e prestadores de serviço, bem como todas as entidades que armazenam, processam ou transmitem os dados do titular do cartão. O PCI DSS compreende um conjunto mínimo de requisitos para proteger os dados do titular do cartão e pode ser aperfeiçoado por controles e práticas adicionais para amenizar os riscos relacionados com leis e normas locais, regionais e do setor. Além disso, os requisitos legais ou regulatórios podem exigir proteção específica de informações pessoalmente identificáveis ou outros elementos de dados (por exemplo o nome do titular do cartão) ou definir práticas de divulgação de uma entidade ligadas a informações de clientes. Os exemplos incluem a legislação relacionada à proteção de dados de clientes, privacidade, roubo de identidade ou segurança de dados. O PCI DSS não sobrepõe as leis locais ou regionais, normas governamentais ou outros requisitos legais. (Requisitos do PCI DSS e Procedimentos da Avaliação segura, 2010).

Abaixo há uma visão geral de alto nível para os 12 requisitos do PCI DSS.

| Padrão de Segurança de Dados do PCI – Visão Geral Alto Nível | |
|---|---|
| **Construir e manter uma rede segura** | 1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão<br>2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança |
| **Proteger os dados do portador do cartão** | 3. Proteger os dados armazenados do titular do cartão<br>4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas |
| **Manter um programa de gerenciamento de vulnerabilidades** | 5. Usar e atualizar regularmente o software ou programas antivírus<br>6. Desenvolver e manter sistemas e aplicativos seguros |
| **Implementar medidas de controle de acesso rigorosas** | 7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio<br>8. Atribuir uma identidade exclusiva para cada pessoa que tenha acesso ao computador<br>9. Restringir o acesso físico aos dados do titular do cartão |
| **Monitorar e testar as redes regularmente** | 10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão<br>11. Testar regularmente os sistemas e processos de segurança |
| **Manter uma política de segurança de informações** | 12. Manter uma política que aborde a segurança das informações para todas as equipes |

Figura 1 - Visão Geral de Alto Nível

Segundo os Requisitos do PCI DSS e Procedimentos da Avaliação da Segurança (CPSLP, 2008), o PCI DSS se aplica onde quer que os dados da conta sejam armazenados, processados ou transmitidos. Os Dados da Conta se consistem em Dados do Titular do cartão mais Dados de autenticação confidenciais, como segue:

| Os Dados do titular do cartão incluem | Os Dados de autenticação confidenciais incluem |
|---|---|
| • o número da conta principal (PAN) | • Dados em tarja magnética ou equivalente em chip |
| • o nome do titular do cartão | • CAV2/CVC2/CVV2/CID |
| • Data de vencimento | • PINs/Bloqueios de PIN |
| • Código de serviço | |

Figura 2 - Dados da Conta

O número da conta principal é o fator decisivo na aplicabilidade dos requisitos do PCI DSS. Os requisitos do PCI DSS são aplicáveis se um número de conta principal (PAN) for armazenado, processado ou transmitido (CPSLP, 2010).

A incorporação do PCI DSS torna – se cada dia mais importante devido ao crescimento do número de dados violados. Segundo o Relatório de Investigação de Violação de Dados da Verizon (2012), realizada em 36 países, as empresas consideradas grandes (empresas com pelo menos 1000 funcionários) do ramo financeiro ou de seguros são responsáveis por 28% dos dados violados em 2011. 96% das empresas vítimas de violação não possuiam o nível exigido pelo PCI DSS em sua última avaliação.

- *Dimensão Operacional da Qualidade*

Segundo Carvalho e Paladini (2012), a visão histórica mais consolidada da qualidade é a sua dimensão operacional. Esta concepção está centrada no fato de que a qualidade deve ser gerada a partir do processo produtivo. Antes que essa visão fosse cristalizada, o esforço dos especialistas na área estava centrado na qualidade do produto. Para tanto, foram desenvolvidos instrumentos de avaliação do produto acabado, por meios de inspeções e análises de amostras. A ineficiência deste procedimento foi percebida rapidamente: a inspeção do produto acabado não tem o poder de alterar a qualidade do próprio produto. Parece óbvio, contudo, que as informações desta inspeção podem ser valiosas para novas ações na fábrica. Ou seja: a inspeção do produto acabado torna–se útil na medida em que transmite as informações obtidas na avaliação para o processo. A avaliação do produto, assim, torna–se fonte de análises para melhorias do processo produtivo. Com efeito, como o produto é resultado do processo, priorizam–se as ações voltadas para o processo produtivo, isto é, para causas e não para efeitos.

Dessa maneira, A ênfase da qualidade no processo centra–se na eliminação de defeitos que ocorrem ao longo de fases bem definidas, que vão desde a percepção dos defeitos, passam pela sua correção e deságuam na eliminação de suas causas (ações preventivas). De certa forma, essa concepção nunca mudou. O que mudou, ao longo do tempo, foi a noção de defeito, hoje inteiramente substituída pelo conceito de perda, muito mais amplo.

## 3. Solução Proposta

O primeiro passo para a solução do problema proposto foi a determinação do escopo de análise em que o FMEA será aplicado. No caso deste trabalho, o escopo inclui todas as exigências impostas pelo Padrão de Segurança de Dados do Setor de cartões de pagamento.

Desta forma, é importante determinar os Sistemas, Subsistemas e Componentes que serão objetos de análise do FMEA.

Segundo Bertalanffy (1973), um sistema é um conjunto de unidades reciprocamente relacionadas tendo dois conceitos:

- Propósito: todo sistema, assim como seus elementos, possuem um objetivo
- Globalismo – todo sistema tem uma natureza orgânica onde qualquer alteração em uma unidade desse sistema afetará o sistema como um todo pois ocorrerá uma encadeamento de acontecimentos.

O objetivo do PCI DSS é fortalecer a segurança das informações nas empresas empregando 12 requisitos. Desta forma, o Sistema PCI DSS será analisado considerando suas unidades. As unidades do PCI DSS serão os 6 grupos que organizam as exigências. Logo, o Sistema PCI DSS é dividido em 6 grupos, que constituem os Subsistemas; por sua vez, esses Subsistemas possuem como Componentes as 12 exigências do PCI DSS, conforme figura 1.

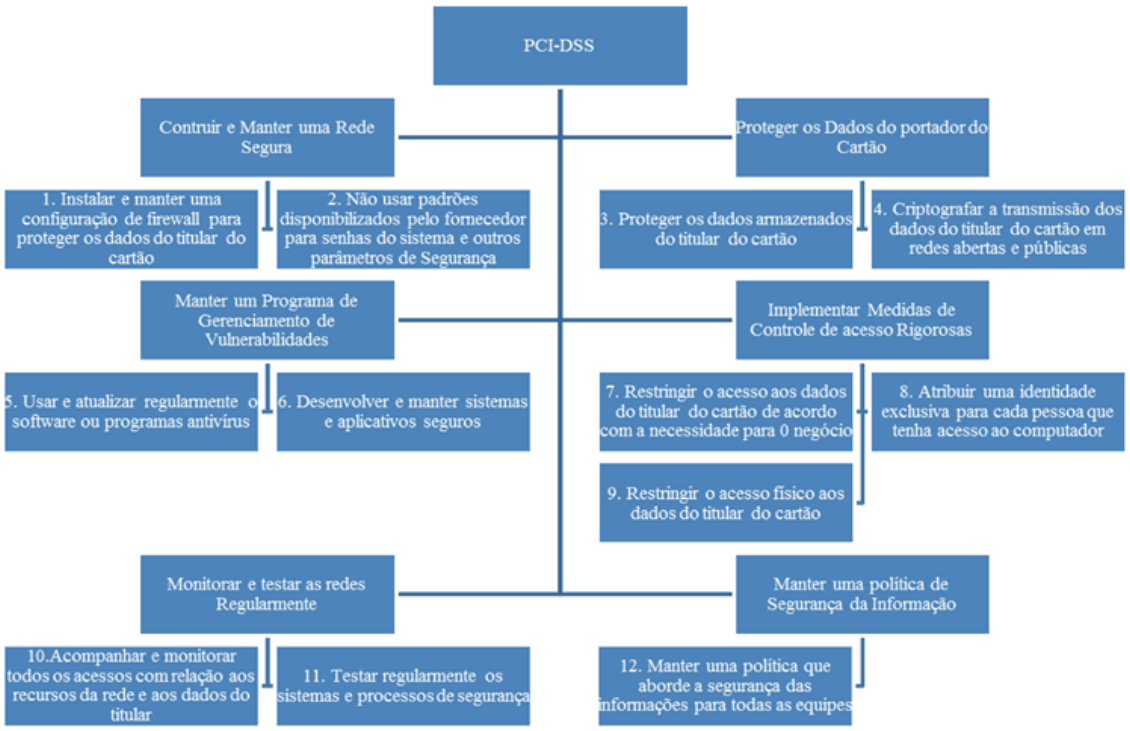


Figura 3 - Sistema, Subsistemas e Componentes da análise

Sendo uma ferramenta que tem como foco a percepção do cliente em relação ao produto a ser entregue, a definição de quem será o cliente do projeto em questão é extremamente importante. O Manual de Referência (IQA, 2008) lista como clientes a serem considerados:

Usuário Final, Montagem OEM e Centros de Fabricação, Fabricação em Cadeia de Suprimento e Reguladores. Para o projeto em questão, os clientes serão:

- Usuário Final, que no contexto deste trabalho será o titular do cartão que deseja poder utilizar o cartão sempre que quiser e com segurança;
- Reguladores, que no contexto desde trabalho será o conselho do Setor de cartões de Pagamento que auditará anualmente a empresa a fim de verificar se todas as exigências são atendidas.

Antes de iniciar o FMEA é importante obter o maior número de informações possíveis para que a compreensão do sistema, subsistema e componentes seja a melhor possível e desta forma gerar os requisitos e características funcionais. No caso deste trabalho as exigências do PCI DSS serão os requisitos funcionais do projeto. Com as informações iniciais definidas, pode–se iniciar o preenchimento do formulário, que será o artefato da análise. Antes de iniciar a análise propriamente dita, é necessário completar o cabeçalho do formulário pois será através dele que será possível identificar o que está sendo analisado. O cabeçalho deste formulário é composto pelos seguintes campos:

- **Sistema**: nome do sistema a ser analisado
- **Subsistema**: nome do subsistema a ser analisado
- **Componente**: nome do componente a ser analisado
- **Equipe Central**: nome dos membros da equipe responsável pelo FMEA
- **Responsabilidade pelo Projeto**: organização e departamento responsável pelo projeto
- **Data Chave**: data limite inicial do FMEA
- **Número FMEA**: sequencia alfanumérica a fim de identificar o documento
- **Elaborado Por**: nome e informações de contato do funcionário responsável pela elaboração do FMEA
- **Data FMEA (Original)**: data original em que o FMEA foi concluído e a última data de revisão

### 3.1 FMEA de Projeto - DFMEA

O primeiro FMEA a ser feito é o DFMEA ou FMEA de Projeto. O Manual de Referência (IQA, 2008) considera que o DFMEA deve contemplar quaisquer modos de falha potencial que possam ocorrer durante o processo de fabricação ou montagem e que estes modos de falha potencial apontados devem ser minimizados ou até mitigados por meio da alteração do projeto. Isto ajuda a situar o momento em que o DFMEA será aplicado. Analisando o projeto em questão, o DFMEA será construído baseado na seguinte pergunta: Como os servidores, switches, firewalls, sistemas, arquiteturas, topologia e demais componentes que processam,

armazenam ou transmitem dados do titular do cartão de pagamento devem ser e que configurações / parametrizações devem possuir para que atendam as exigências do PCI DSS? É importante ter em mente que o DFMEA apoiará o processo de construção e montagem do ambiente que será escopo de certificação.

Com estas informações em mãos tem início o DFMEA. O corpo do formulário DFMEA é composto por campos que darão a orientação necessária para o correto preenchimento do formulário. O significado de cada campo deve estar claro e bem conceituado para que o DFMEA seja feito de forma correta. A seguir, estes campos serão apresentados:

- **Item:** Este campo deverá conter os itens que serão analisados. No contexto deste trabalho, os itens serão os hosts, switches, firewalls, sistemas operacionais e qualquer outro componente do ambiente escopo de certificação que poderá falhar. O Manual de Referência (2008) chama a atenção para que os termos utilizados neste campo estejam de acordo com os demais documentos do projeto para que a rastreabilidade seja assegurada.

- **Função:** Este campo é utilizado para dar uma breve descrição das funções que o item analisado possui e que sejam necessárias para atender o objetivo do projeto.

- **Requisito:** Esta coluna tem como objetivo refinar a análise, pois dará mais informações de como o item analisado deverá atender o objetivo do projeto.

- **Modo de Falha Potencial:** o Modo de Falha Potencial é a maneira de como o item sendo analisado poderia potencialmente falhar em atender as funções e requisitos descritos nas colunas anteriores. A palavra potencial é usada, pois para efetuar a analise é assumida a hipótese de que a falha poderia ocorrer, mas pode não ocorrer necessariamente.

- **Efeito Potencial da Falha:** Este campo deverá ser utilizado para descrever quais os efeitos da falha. Os efeitos devem ser descritos na forma que o cliente definido anteriormente perceberia esta falha.

- **Severidade:** No campo Severidade deverá ser dado um valor relativo de 1 a 10 para o efeito mais grave para o modo de falha definido anteriormente. Os critérios de avaliação sugeridos pelo Manual de Referência foram adaptados para que atendessem o contexto do projeto e são apresentados na figura 4.

| SEVERIDADE | | |
|---|---|---|
| **Efeito** | **Critérios** | **Classificação** |
| Falha em Atender Requisitos de Segurança e / ou Regulatórios | Modo de Falha potencial afeta a operação do ambiente de produção ou envolve não conformidade com regulamentação, sem aviso prévio. | **10** |
| | | **9** |
| Perda ou Degradação de Função Primária | Perda da função primária | **8** |
| | Degradação da função primária | **7** |
| Perda ou Degradação de Função Secundária | Perda da função secundária | **6** |
| | Degradação da função secundária | **5** |
| Incômodo | Degradação perceptível | **4** |
| | Degradação eventualmente perceptível | **3** |
| | Degradação praticamente imperceptível | **2** |
| Nenhum Efeito | Nenhum efeito perceptível | **1** |

Figura 4 - Critérios de Avaliação para Severidade

- **Causa Potencial da Falha:** Este campo é utilizado para descrever as circunstâncias que induziram ou ativaram a falha.

- **Ocorrência:** No campo ocorrência deverá ser dado um valor de 1 a 10 que determinará a probabilidade relativa da causa potencial da falha ocorrer. Os critérios de avaliação indicados pelo Manual de Referência (IQA, 2008) foram utilizados integralmente neste caso e são apresentados na figura 5.

| OCORRÊNCIA | | |
|---|---|---|
| **Probabilidade da falha** | **Critérios** | **Classificação** |
| Muito Alta | Nova Tecnologia / novo projeto, sem histórico. | **10** |
| Alta | A falha é inevitável, com novo projeto / nova aplicação, ou alteração no ciclo de condições operacionais. | **9** |
| | A falha é provável, com novo projeto / nova aplicação, ou alteração no ciclo de condições operacionais. | **8** |
| | A falha é incerta, com novo projeto / nova aplicação, ou alteração no ciclo de condições operacionais. | **7** |
| Moderada | Falhas frequentes associadas a projetos similares, ou simulação e testes de projeto. | **6** |
| | Falhas ocasionais associadas a projetos similares, ou simulação e testes de projeto. | **5** |
| | Falhas isoladas associadas a projetos similares, ou simulação e testes de projeto | **4** |
| Baixa | Somente falhas isoladas, associadas a projetos praticamente idênticos, ou em simulação e testes de projeto. | **3** |
| | Falhas não observadas, associadas a projetos praticamente idênticos, ou em simulação e testes de projeto. | **2** |
| Muito Baixa | A falha é eliminada por controle preventivo | **1** |

Figura 5 - Critérios de Avaliação para Ocorrência de Falha

- **Controles Atuais de Projeto:** os Controles Atuais do Projeto estão divididos em dois tipos:
    - *Controle de Prevenção:* são os controles que estão implantados no momento da análise que previnem o modo de falha ou reduz a sua chance de ocorrência.
    - *Controle de Detecção:* são os controles implantados no momento da análise que detectam a existência da causa pelo qual o modo de falha ocorre.
- **Detecção:** neste campo deve ser colocado um valor relativo de 1 a 10 que reflita o melhor controle de detecção atualmente implantando. Para isso, usa – se os seguintes Critérios de Avaliação adaptados do Manual de Referência (IQA, 2008), apresentados na figura 5.

| DETECÇÃO | | | |
|---|---|---|---|
| **Oportunidade para Detecção** | **Critérios** | **Classificação** | **Probabilidade de Detecção** |
| Nenhuma oportunidade de detecção | Não pode detectar ou o resultado não foi verificado, com certeza absoluta de não detecção | 10 | Praticamente Impossível |
| Improvável detectar em qualquer estágio | O controle é alcançado somente com a verificação aleatória, tendo possibilidades de não detecção | 9 | Muito Remota |
| Após o congelamento do projeto, antes de ir a produção | O controle é alcançado somente com inspeção visual, tendo pouca chance de detecção | 8 | Remota |
| | Controles têm pouca chance de detecção | 7 | Muito Baixa |
| | Controles podem detectar anomalias | 6 | Baixa |
| Antes do congelamento do projeto (Testes) | Controles detectam anomalias na fase de validação final do produto (testes de desenvolvimento ou validação) | 5 | Moderada |
| | Controles têm boas chances para detectar durante a fase de validação do produto (testes de desenvolvimento ou validação). | 4 | Moderadamente Alta |
| | Controles têm boas chances para detectar durante a fase de validação do produto (testes de desenvolvimento ou validação) em fase inicial de testes. | 3 | Alta |
| Detecção em estágio de planejamento | Os controles de análise / detecção de projeto têm uma forte capacidade de detecção. | 2 | Muito Alta |
| Detecção não aplicável. Prevenção de Falha | A causa de falha ou modo de falha não pode ocorrer porque foi totalmente prevenida através de soluções de projeto (padrão comprovado, melhores práticas, etc.) | 1 | Praticamente Certa |

Figura 3 - Critérios de Avaliação para detecção

- **Número de Prioridade de Risco (NPR):** o NPR é obtido da seguinte forma:

NPR = Severidade X Ocorrência X Detecção

Como o próprio nome diz, o NPR é utilizado para ajudar a priorizar as ações. Todavia o Manual de Referência (IQA, 2008) chama a atenção que a utilização do NPR para determinar a necessidade de uma ação não é recomendada e deve – se olhar as classificações de Severidade, Ocorrência e Detecção separadamente para que seja determinada a necessidade de ação.

- **Ações Recomendadas:** Neste campo deve – se colocar as ações recomendadas para que as classificações com maiores valores atribuídos sejam reduzidos.

- **Responsabilidade e Data de Conclusão:** Este campo é utilizado para se colocar quem será o responsável por implantar as Ações Recomendadas, e a Data de Conclusão desta atividade.

- **Ações Implementadas:** Neste campo coloca – se uma breve descrição das ações que foram implementadas.

- **Severidade, Ocorrência, Detecção e NPR:** Após as ações corretivas tomadas, é feita uma nova classificação a fim de verificar se estas ações resultaram na redução ou até na mitigação do risco.

Abaixo segue o desenvolvimento do DFMEA para os Requisito 1 e 2 do PCI-DSS. Importante destacar que os mesmos diagramas foram elaborados para todos os requisitos do PCI-DSS.

## Análise de Modo e Efeito de Falha Potencial (FMEA de Projeto)
## DFMEA

Sistema: PCI-DSS | Responsabilidade pelo Projeto: | Número FMEA:
Subsistema: Construir e Manter uma Rede Segura | Data-Chave: | Elaborado Por:
Componente: Instalar e manter uma configuração de Firewall | Data FMEA (Original):
Equipe Central:

NPR 200 -
NPR 100 - 199
NPR 1-99

| | | | | | | | Projeto Atual | | | | | | Resultado das Ações | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ITEM | FUNÇÃO | REQUISITO | MODO DE FALHA POTENCIAL | EFEITO POTENCIAL DA FALHA | SEVERIDADE | CAUSA POTENCIAL DA FALHA | CONTROLES Prevenção | OCORRÊNCIA | CONTROLES Detecção | DETECÇÃO | NPR | AÇÃO RECOMENDADA | Responsabilidade e Data de Conclusão | Ações Implementadas | SEVERIDADE | OCORRÊNCIA | DETECÇÃO | NPR |
| Firewall | Analisar o tráfego de rede e bloquear as transmissões que não atendam as regras previamente estabelecidas | Proteger o acesso não autorizado com origem em redes não confiável, independendo do modo de acesso (Exemplos:Internet, e - commerce, conexão dedicada, redes sem fio, entre outras) | Acesso indevido ao ambiente de dados do portador de cartão, originado de rede não confiável | Acesso a dados sigilosos, como os do titular do cartão.<br><br>Vazamento de informações sigilosas e do titular do cartão.<br><br>Alteração de parâmetros de configuração.<br><br>Perda de informação sensível ao negócio.<br><br>Acesso ao banco de dados que contém os dados do titular do cartão | 9 | A rede do ambiente protegido não está segmentada por uma DMZ e/ou protegida por um firewall | Regras de firewall restringem os acessos pela origem e destino do pacote | 4 | Verificação manual dos logs do firewall | 6 | 216 | Segmentar a rede do ambiente que contém os dados do titular do cartão, disponibilizando um firewall em cada conexão da internet e entre qualquer zona desmilitarizada (DMZ) e a zona da rede interna conforme requisito 1.1.3 do PCI-DSS v2.0 | Dep. Infraestrutura e Dep. Segurança da Informação | Rede segmentada, incluindo a DMZ, protegida por firewall | 9 | 3 | 3 | 81 |
| | | | | | | Acesso indevido pois o tráfego de dados não está limitado ao necessário para o ambiente de dados do portador do cartão | Verificação isolada efetuada pelo funcinário | 5 | Verificação manual dos logs do firewall<br><br>Indisponibilidade do serviço | 6 | 270 | Restringir o tráfego de entrada e saída para aquele que é necessário para o ambiente de dados do portador do cartão conforme requisito 1.2.1 do PCI-DSS v2.0 | Dep. Segurança da Informação | Regras de firewall construídas limitando o tráfego para somente o necessário para o ambiente do portador do cartão | 9 | 3 | 3 | 81 |
| | | | | | | Acesso indevido pois o ambiente de dados do portador do cartão está acessível através de acesso público direto | Verificação isolada efetuada pelo funcinário | 5 | Verificação manual dos logs do firewall<br><br>Indisponibilidade do serviço | 6 | 270 | Implementar uma DMZ para limitar o tráfego somente a componentes do sistema que oferece serviços, protocolos e porta acessíveis publicamente, limitar o tráfego de entrada da Internet a endereços IP na DMZ, não permitir rotas diretas entre a internet e o ambiente protegido conforme requisitos 1.3.1, 1.3.2 e 1.3.3 do PCI-DSS v2.0 | Dep. Segurança da Informação | Segmentação da rede do ambiente de dados do portador do cartão, criando assim uma DMZ | 9 | 2 | 3 | 54 |
| | | | | | | O atacante teve acesso ao ambiente de dados de portador de cartão pois teve acesso aos endereços internos da rede | Verificação isolada efetuada pelo funcinário | 5 | Verificação manual dos logs do firewall | 6 | 270 | Não permitir que endereços internos sejam transmitidos via internet na DMZ conforme requisito 1.3.4 do PCI-DSS v2.0 | Dep. Segurança da Informação | Regras de firewall negando a saída direta de endereços internos. | 9 | 2 | 3 | 54 |
| | | | | | | O acesso ao ambiente de dados de portador de cartão foi feito através de uma sessão aberta por FTP onde o firewall não efetuou inspeção dinâmica das portas abertas por este protocolo | Verificação isolada efetuada pelo funcinário | 5 | Verificação manual dos logs do firewall | 6 | 270 | Implementar inspeção com status, também conhecida por filtragem dinâmica de pacotes, conforme requisito 1.3.6 do PCI-DSS v2.0 | Dep. Segurança da Informação | Implantação de firewall capaz de realizar inspeção dinamica de pacotes e verificar se a funcionalidade está habilitada | 9 | 2 | 2 | 36 |
| | | | Acesso a base de dados de portador de cartão | Acesso a dados sigilosos, como os do titular do cartão.<br><br>Vazamento de informações sigilosas e do titular do cartão.<br><br>Perda de informação sensível ao negócio. | 9 | O servidor de banco de dados situa - se na DMZ | ND | 6 | ND | 6 | 324 | Implementar os componentes do sistema que armazenam dados do titular do cartão em uma zona da rede interna, separada da DMZ e de outras redes não confiáveis conforme requisito 1.3.7 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Banco de dados implementado em rede distinta e protegido por firewall | 9 | 3 | 3 | 81 |
| | | | Vazamento de dados do titular do cartão | Acesso a dados sigilosos, como os do titular do cartão.<br><br>Vazamento de informações sigilosas e do titular do cartão.<br><br>Perda de informação sensível ao negócio. | 9 | As regras do firewall não previne o tráfego de saída que não deveria ser autorizado. | Verificação isolada das regras de firewall efetuada pelo funcinário | 5 | Verificação manual dos logs do firewall | 6 | 270 | Não permitir o tráfego de saída não autorizado do ambiente de dados do cartão para a internet conforme requisito 1.3.5 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Regras de firewall parametrizadas para que o tráfego de saída só seja permitido para serviços que apoiam o negócio | 9 | 3 | 3 | 81 |
| | | | Acesso indevido ao ambiente de dados do portador de cartão, originado da rede interna por usuário mal intencionado | Acesso a dados sigilosos, como os do titular do cartão.<br><br>Vazamento de informações sigilosas e do titular do cartão.<br><br>Alteração de parâmetros de configuração.<br><br>Perda de informação sensível ao negócio. | 9 | O ambiente não possui firewall implementado entre a rede protegida e a rede interna | Controle de Acesso no nível usuário | 4 | Verificação manual dos logs do firewall e dos ativos de rede | 6 | 216 | Segmentar a rede do ambiente que contém os dados do titular do cartão, disponibilizando um firewall em cada conexão da internet e entre qualquer zona desmilitarizada (DMZ) e a zona da rede interna conforme requisito 1.1.3 do PCI-DSS v2.0 | Dep. Infraestrutura e Dep. Segurança da Informação | Rede segmentada | 9 | 2 | 3 | 54 |
| | | | Acesso indevido ao ambiente de dados do portador de cartão, originado de rede sem fio | Acesso a dados sigilosos, como os do titular do cartão.<br><br>Vazamento de informações sigilosas e do titular do cartão.<br><br>Alteração de parâmetros de configuração.<br><br>Perda de informação sensível ao negócio. | 9 | O ambiente não possui firewall de perímetro entre redes sem fio e o ambiente de dados do portador do cartão | ND | 5 | Verificação manual dos logs dos ativos de rede<br><br>Enventual indisponibilidade do ambiente de produção | 7 | 315 | Instalar firewalls de perímetro entre as redes sem fio e o ambiente de dados do portador do cartão, recusando ou controlando (no caso de necessidade comercial) o tráfego a partir do ambiente sem fio conforme requisito 1.2.3 do PCI-DSS v2.0 | Dep. Infraestrutura e Dep. Segurança da Informação | Implantação de firewall entre as redes sem fio e o ambiente de dados do portador do cartão | 9 | 3 | 3 | 81 |

Figura 6 - DFMEA Requisito 1 PCI DSS

## Análise de Modo e Efeito de Falha Potencial (FMEA de Projeto)
## DFMEA

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sistema | PCI-DSS | | Responsabilidade pelo Projeto | | | | Número FMEA | | | | NPR 200 - | | | | | | | | |
| Subsistema | Construir e Manter uma Rede Segura | | Data-Chave | | | | Elaborado Por | | | | NPR 100 - 199 | | | | | | | | |
| Componente | Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança | | | | | | Data FMEA (Original) | | | | NPR 1-99 | | | | | | | | |
| Equipe Central | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | Projeto Atual | | | | | | | | | Resultado das Ações | | |
| ITEM | FUNÇÃO | REQUISITO | MODO DE FALHA POTENCIAL | EFEITO POTENCIAL DA FALHA | SEVERIDADE | CAUSA POTENCIAL DA FALHA | CONTROLES Prevenção | OCORRÊNCIA | CONTROLES Detecção | DETECÇÃO | NPR | AÇÃO RECOMENDADA | Responsabilidade e Data de Conclusão | Ações Implementadas | SEVERIDADE | OCORRÊNCIA | DETECÇÃO | NPR |
| Roteador de Redes Sem Fio | Prover acesso a dispositivos através de redes sem fio | Oferecer mobilidade para funcionários que possuam dispositivos móveis | Acesso a rede da empresa efetuado por pessoa não autorizada através da rede sem fio | Vazamento de dados sigilosos.<br><br>Perda de dados sigilosos.<br><br>Alteração de parâmetros de configuração.<br><br>Indisponibilidade do serviço de processamento de cartões | 9 | Roteador foi instalado sem que as configurações padrão do fabricante fossem alteradas, permitindo assim que o atacante tivesse acesso ao dispositivo em questão | ND | 7 | Verificação dos logs de acesso do roteador sem fio | 6 | 378 | Em ambiente sem fio conectados ao ambiente de dados do portador de cartão, alterar os padrões do fornecedor, conforme requisito 2.1.1 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | As senhas de acesso ao dispositivo, bem como os demais parâmetros de segurança do equipamento foram alterados para valores diferentes do fornecido pelo fabricante | 9 | 1 | 3 | 27 |
| Servidores | Abrigar o sistema operacional e as funções / serviços que forem definidos | O servidor deverá funcionar sem interrupções e as funções / serviços instalados nele devem estar seguras | Acesso não autorizado ao banco de dados que abriga os dados de portador do cartão | Comprometimento dos dados do portador do cartão | 8 | A função de banco de dados está implementada juntamente da função de servidor de WEB | Proteção do ambeinte é feita pelo firewall | 5 | Verificação manual dos logs dos servidores e do firewall | 5 | 200 | Implementar somente uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor conforme requisito 2.2.1 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Servidor de WEB instalado outro servido, contendo somente a função WEB | 8 | 2 | 2 | 32 |
| | | | Acesso não autorizado ao ambiente de dados do portador do cartão | Vazamento de dados sigilosos.<br><br>Comprometimento do dados do portador do cartão<br><br>Perda de dados sigilosos.<br><br>Alteração de parâmetros de configuração.<br><br>Indisponibilidade do serviço de processamento de cartões | 9 | O ambiente foi acessado através da feature de file-sharing habilitada no servidor WEB | Proteção do ambeinte é feita pelo firewall | 5 | Verificação manual dos logs dos servidores e do firewall | 5 | 225 | Ativar somente serviços, protocolos, daemons, etc, necessários e seguros, conforme exigido para a função do sistema, conforme requisito 2.2.2 e 2.2.4 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Desenvolvido Hardening (Padrão de configuração de segurança) para os servidores WEB, desabilitando os serviços não seguros e desnecessários | 8 | 3 | 3 | 72 |
| | | | | | | O ambiente foi acessado através de ataque Man In The Middle (MITM) pois a conexão remota aos servidores do ambiente de dados do portador do cartão não era criptografada | Seleção manual da opção de conexão criptografada pelo operador | 4 | Verificação manual dos logs dos servidores e do firewall | 5 | 180 | Criptpgrafar todo o acesso administrativo não console durante a conexão, conforme requisito 2.3 do PCI-DSS v2.0.<br><br>Configurar parâmetros de segurança do sistema para impedir uso incorreto conforme requisito 2.2.3 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Desenvolvido Hardening (Padrão de configuração de segurança) para os servidores WEB, desabilitando os serviços não seguros e desnecessários<br><br>Opção de conexão criptografada tornada padrão | 9 | 2 | 2 | 36 |
| Provedor de Hospedagem | Hospedar os servidores, dispositivos de rede e demais equipamentos necessários para a operação do negócio | Fornecer hospedagem, energia redundante, climatização e segurança física aos equipamentos da empresa | Acesso físico por pessoa não autorizada ao ambiente de dados do portador do cartão | Vazamento de dados sigilosos.<br><br>Comprometimento do dados do portador do cartão<br><br>Perda de dados sigilosos.<br><br>Alteração de parâmetros de configuração.<br><br>Indisponibilidade do serviço de processamento de cartões | 9 | Ambiente acessado fisicamente pois o provedor de hospegem não verificou se a pessoa possuia autorização para acessar tal ambiente | Fechaduras dos Racks | 5 | Verificação in loco do ambiente de dados do portador do cartão | 6 | 270 | de hospedagem compartilhada que protejam o ambiente hospedado conforme requisito 2.4, A1.1 e A1.4 do PCI-DSS v2.0 | Dep. Segurança da Informação, Jurídico | Contratação de provedor de hospedagem com certificação PCI-DSS | 9 | 2 | 2 | 36 |

Figura 7 - DFMEA Requisito 2 PCI DSS

### 3.2 FMEA de Processo – PFMEA

Após efetuar o FMEA de Projeto, deve ser feito o FMEA de Processo e, neste caso, alguns itens analisados no DFMEA servirão de entrada para o PFMEA pois serão utilizados como entrada para alguns processos no desenvolvimento do produto.

O formulário de análise do FMEA de Processo tem seu preenchimento praticamente igual ao do FMEA de Projeto. Na realidade, somente o campo Item é alterado para Etapa do Processo. Neste caso, o Modo de falha potencial será analisado de forma que se verifiquem as maneiras pela qual o processo citado poderá potencialmente falhar. Desta forma, o preenchimento do formulário PFMEA seria feito conforme os exemplos abaixo para os Requisitos 1 e 2 do PCI DSS:

# Análise de Modo e Efeito de Falha Potencial (FMEA de Processo)
# PFMEA

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sistema | PCI-DSS | Responsabilidade pelo Projeto | | | | | | | Número FMEA | | | | | | | | | | |
| Subsistema | Contruir e manter uma rede Segura | Data-Chave | | | | | | | Elaborado Por | | | | | | | | | | |
| Componente | Instalar e manter uma configuração de Firewall | | | | | | | | Data FMEA (Original) | | | | | | | | | | |
| Equipe Central | | | | | | | | | | | | | | | | | | | |
| | | | | | | Projeto Atual | | | | | | | | | | Resultado das Ações | | | |
| ETAPA DO PROCESSO/ ITEM | REQUISITO | MODO DE FALHA POTENCIAL | EFEITO POTENCIAL DA FALHA | SEVERIDADE | CAUSA POTENCIAL DA FALHA | CONTROLES Prevenção | OCORRÊNCIA | CONTROLES Detecção | DETECÇÃO | NPR | AÇÃO RECOMENDADA | Responsabilidade e Data de Conclusão | Ações Implementadas | SEVERIDADE | OCORRÊNCIA | DETECÇÃO | NPR |
| Manutenção de Regras de Firewall | Incluir, Alterar ou Excluir regras de firewall conforme necessidade do negócio | Acesso indevido ao ambiente de dados do portador do cartão | Acesso a dados sigilosos, como os do titular do cartão.<br><br>Vazamento de informações sigilosas e do titular do cartão.<br><br>Alteração de parâmetros de configuração.<br><br>Perda de informação sensível ao negócio.<br><br>Acesso ao banco de dados que contém os dados do titular do cartão | 9 | O acesso indevido foi feito através de uma regra que não era mais necessária e não foi removida ou desabilitada | Verificação isolada efetuada pelo funcinário | 5 | Verificação manual dos logs do firewall | 7 | 315 | Analisar os conjuntos de regras de firewall pelo menos semestralmente conforme requisito 1.1.6 do PCI-DSS v2.0 | Dep. Infraestrutura e Dep. Segurança da Informação | Instituição de análise semestral do conjunto de regras de firewall | 9 | 3 | 3 | 81 |
| | | | | | Alteração de regra de firewall com o parâmetrização incorreta | Verificação isolada efetuada pelo funcinário | 5 | Eventual indisponibilidade do serviço que depende da regra | 7 | 315 | Instituir um processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do Firewall conforme requisito 1.1.1 do PCI-DSS v2.0<br><br>Construir um diagrama de rede com todas as conexões com relação aos dados do portador do cartão conforme requisito 1.1.2 do PCI-DSS v2.0 | Dep. Segurança da Informação | Processo de Gestão de Mudanças de Regras de Firewall e Teste de Intrusão implementados<br><br>Criação do Diagrama de Rede. | 9 | 3 | 3 | 81 |
| | | | | | Alteração de regra de firewall sem autorização | ND | 5 | Eventual indisponibilidade do serviço que depende da regra | 7 | 315 | Instituir um processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do Firewall conforme requisito 1.1.1 do PCI-DSS v2.0 | Dep. Segurança da Informação | Processo de Gestão de Mudanças de Regras de Firewall e Teste de Intrusão implementados | 9 | 3 | 3 | 81 |
| | | | | | Após a implantação da(s) regra(s) de firewall, estas não foram testadas | Verificação isolada efetuada pelo funcinário | 5 | Eventual indisponibilidade do serviço que depende da regra | 7 | 315 | Instituir um processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do Firewall conforme requisito 1.1.1 do PCI-DSS v2.0 | Dep. Segurança da Informação | Processo de Gestão de Mudanças de Regras de Firewall e Teste de Intrusão implementados | 9 | 3 | 3 | 81 |
| | | | | | Alteração de regra de firewall permitiu que os endereços internos fossem visíveis pela internet | Verificação isolada efetuada pelo funcinário | 5 | Verificação manual dos logs do firewall | 7 | 315 | Instituir um processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do Firewall conforme requisito 1.1.1 do PCI-DSS v2.0 e não permitir que endereços internos sejam transmitidos via internet conforme rquisito 1.3.4 do PCI-DSS v2.0 | Dep. Segurança da Informação | Processo de Gestão de Mudanças de Regras de Firewall e Teste de Intrusão implementados | 9 | 2 | 3 | 54 |
| | | | | | Os endereços privados foram divulgados para partes que não fazem parte do negócio após implantação de nova regra de firewall | Verificação isolada efetuada pelo funcinário | 5 | Verificação manual dos logs do firewall | 7 | 315 | Não divulgar endereços IP privados e informações de roteamento conforme requisito 1.3.8 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Endereços IP privados camuflados através de NAT | 9 | 2 | 3 | 54 |
| | | Acesso aos dispositivos de rede efetuado por usuário interno não autorizado | Indisponibilidade do ambiente que suporta o serviço de processamento de cartões.<br><br>Alteração de parâmetros de forma indevida e não autorizada. | 8 | Permissão de acesso aos dispositivos de rede foi dada a um usuário que não deveria ter acesso a tais dispositivos | Verificação isolada efetuada pelo funcinário | 5 | Verificação manual dos usuários | 5 | 200 | Manter um registro dos grupos, funções e responsabilidades quanto ao gerenciamento lógico dos componentes de rede conforme requisito 1.1.4 do PCI-DSS v2.0 | Dep. Segurança da Informação | Criação dos registros conforme requisito/. | 8 | 2 | 2 | 32 |
| | | Indisponibilidade de um ou mais dispositivos de rede. | Indisponibilidade do ambiente que suporta o serviço de processamento de cartões. | 8 | Após falha de determinado dispositivo de rede, o arquivo de configuração de backup utilizado para configurar o novo dispositivo não continha todas as configurações que o dispositivo em falha possuia | Backup esporádico dos arquivos de configuração | 4 | Configuração esporádica dos dispositivos de backup | 5 | 160 | Proteger e sincronizar os arquivos de configuração do dispositivo de rede conforme requisito 1.2.2 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Instituição de processo que copia e aplica a nova configuração em dispositivos de backup | 8 | 2 | 2 | 32 |

Figura 8 - PFMEA Requito 1 PCI DSS

Análise de Modo e Efeito de Falha Potencial (FMEA de Processo)
PFMEA

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sistema | PCI-DSS | Responsabilidade pelo Projeto | | | | Número FMEA | | | | | | | | | | |
| Subsistema | Controle e manter uma rede Segura | Data-Chave | | | | Elaborado Por | | | | | | | | | | |
| Componente | Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros | | | | | Data FMEA (Original) | | | | | | | | | | |
| Equipe Central | | | | | | | | | | | | | | | | |
| | | | | | | Projeto Atual | | | | | | | | Resultado das Ações | | |
| ETAPA DO PROCESSO/ ITEM | REQUISITO | MODO DE FALHA POTENCIAL | EFEITO POTENCIAL DA FALHA | SEVERIDADE | CAUSA POTENCIAL DA FALHA | CONTROLES Prevenção | OCORRÊNCIA | CONTROLES Detecção | DETECÇÃO | NPR | AÇÃO RECOMENDADA | Responsabilidade e Data de Conclusão | Ações Implementadas | SEVERIDADE | OCORRÊNCIA | DETECÇÃO | NPR |
| Administração remota do ambiente de dados do portador de cartão | Deve ser possível efetuar a administração do ambiente de dados do portador de cartão de forma remota e segura | Acesso não autorizado ao ambiente de dados do portador do cartão | Vazamento de dados sigilosos.<br><br>Comprometimento do dados do portador do cartão<br><br>Perda de dados sigilosos.<br><br>Alteração de parâmetros de configuração.<br><br>Indisponibilidade do serviço de processamento de cartões | 9 | O ambiente foi acessado através de ataque Man In The Middle (MITM) pois a conexão remota aos servidores do ambiente de dados do portador do cartão não era criptografada | Seleção manual da opção de conexão criptografada pelo operador | 4 | Verificação manual dos logs dos servidores e do firewall | 5 | 180 | Criptpgrafar todo o acesso administrativo não console durante a conexão, conforme requisito 2.3 do PCI-DSS v2.0.<br><br>Configurar parâmetros de segurança do sistema para impedir uso incorreto conforme requisito 2.2.3 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Desenvolvido Hardening (Padrão de configuração de segurança) para os servidores WEB, desabilitando os serviços não seguros e desnecessários<br><br>Opção de conexão criptografada tornada pardrão | 9 | 2 | 2 | 36 |
| Manutenção da Segurança dos compoentes do ambiente de dados do portador de cartão | Manter os componetes do ambiente de dados do portador do cartão sempre seguros, comas últimas atualizações fornecidas pelos fabricantes | Acesso não autorizado ao ambiente de dados do portador do cartão | Vazamento de dados sigilosos.<br><br>Comprometimento do dados do portador do cartão<br><br>Perda de dados sigilosos.<br><br>Alteração de parâmetros de configuração.<br><br>Indisponibilidade do serviço de processamento de cartões | 9 | O ambiente foi acessado por falta de aplicação de patch de segurança do sistema operacional Windows Server 2008 R2 | Atualização esporádica dos patches de segurança e correção de bugs. | 5 | Notificação do próprio sistema operacional. Notificação externa através da assintura de listas | 3 | 135 | 2.2 e 6.2 do PCI-DSS v2.0 | Dep. Segurança da Informação e Dep. De Infraestrutura | Implantação da Política de Gestão de patches de correção e de segurança | 9 | 2 | 3 | 64 |

Figura 9 - PFMEA Requisito 2 PCI DSS

## 4. Resultados obtidos

Uma grande contribuição do FMEA é o fato desta ser uma ferramenta multidisciplinar e exigir a participação de todas as áreas funcionais na análise. Isso faz com que o conhecimento absorvido durante a análise por seus participantes seja maior que no processo normal de análise de gaps e plano de ação além de deixar este conhecimento documentado, ou seja, é um processo onde tanto colaboradores, quanto a empresa ganham.

Outro ponto de grande valia para a empresa é o fato de que o uso do FMEA proporciona a oportunidade de identificar modos de falha que resultam em um mesmo efeito potencial. Isso faz com que sejam descobertos inter-relações entre processos, itens e entre processos e itens que ainda não haviam sido mapeados.

Como o FMEA deve ser considerado um documento vivo, onde todas as ações preventivas / corretivas devem ser acompanhadas, a sua adoção torna – se uma ferramenta importante para melhoria contínua, pois este acompanhamento proporciona a oportunidade de identificar os pontos onde o produto pode melhorar.

Os pontos acima citados são componentes indispensáveis para a Gestão da Segurança da Informação em qualquer empresa. Saber como e contra quem se prevenir faz com que a área de Segurança da Informação foque seus esforços de forma mais efetiva e alinhada ao negócio.

Em relação a certificação PCI DSS, o FMEA fornece uma forma organizada e efetiva de acompanhar a aderência da empresa às exigências do conselho, facilitando desta forma o processo de certificação anual.

Com o passar do tempo, a adoção do FMEA gera análises cada vez mais robustas, pois ele pode ser utilizado como ponto de partida para projetos parecidos, fornecendo assim uma base sólida de conhecimento e naturalmente um produto mais maduro e confiável.

## Referências

BERTALANFFY, Ludwig Von. **Teoria Geral de Sistemas.** Vozes, 1973.

CARVALHO, M.M.; PALADINI, E.P. **Gestão da Qualidade – Teoria e Casos**. Elsevier, 2ª Edição, 2012.

CPSLP - CONSELHO DE PADRÕES DE SEGURANÇA LLC DO PCI **Requisitos do PCI DSS e Procedimentos da Avaliação da Segurança**. PCI Security Standards Council. 2ª versão, 2010.

IQA – INSTITUTO DA QUALIDADE AUTOMOTIVA. **Análise de Modo e Efeitos de Falha Potencial – Manual de Referência.** Automotive Industry Action Group, 4ª Edição, 2008.

STAMATIS, D. H. **Failure Mode and Effect Analysis.** ASQ Quality Press, 2ª Edição, 2003.

VERIZON. **Data Breach Investigations Report**. Ed. Verizon, 2012.