

## Estudo de Caso

Este texto é a base do Estudo de Caso a ser realizado durante a disciplina de Gestão da Segurança da Informação. Os passos a serem realizados, e documentados nas folhas do final da apostila são:

1. Definição de um Critério de Aceitação do Risco, com base na documentação do anexo 1 (Página 79) e as orientações disponíveis no slide da página 22 do material teórico;
2. Mapeamento dos Riscos no Processo ilustrado no Caso. Com base na figura 1, identificar:
  - a) Ativos físicos, tecnológicos e humanos;
  - b) Vulnerabilidades e ameaças aos ativos;
  - c) Elaborar um esboço das ferramentas de análise, mensurando qualitativamente impactos decorrentes de cada ataque (ameaça + vulnerabilidade) com a tabela fornecida.
    - i. CIDAL; e a seguir,
    - ii. GUT.
3. Avaliação dos Riscos - Comparar resultados com os Critérios de Aceitação do Risco
4. Propor ações de Política de Segurança e de Continuidade dos Negócios onde cabível, identificando as estratégias de tratamento do Risco adotadas:
  - a. Modificar;
  - b. Reter;
  - c. Evitar ou
  - d. Compartilhar. Também é possível combinar estas ações.

Para simplificar, vamos considerar que todos os ataques têm a mesma probabilidade de ocorrência.

O Case a ser ilustrado a seguir foi modelado em BPMN (*Business Process Modelling Notation*) e é baseado no artigo “*Towards Definition of Secure Business Processes*”, de Olga Altuhhova, Raimundas Matulevičius e Naved Ahmed, publicado no livro *Advanced Information Systems Engineering Workshops*, da editora Springer Berlin Heidelberg, pg 1-15, e disponível em <http://gsya.esi.uclm.es/WISSE2012/papers/paper5.pdf>. Trata-se de uma Loja Virtual, com a abstração necessária para viabilizar o exercício dos passos da metodologia proposta na apresentação da disciplina com objetividade e rapidez. Como em inúmeras empresas atuais, os negócios de varejo realizados online possuem movimentação bem maior do que a física, fazendo com que estas lojas abandonem ou minimizem ao máximo suas operações de venda física. Amazon, Submarino e Shoptime já são assim, e outras tradicionalmente físicas, como as Casas Bahia, Magazine Luiza, Ponto Frio e Walmart vem investindo pesado em suas plataformas B2C<sup>1</sup>. No caso ilustrado, a falta de planejamento, de envolvimento de todos os setores e principalmente dos especialistas em TI provocou o lançamento de uma plataforma problemática, sujeita a ataques por usar códigos antigos já prontos e não verificados. Infelizmente, isso só pôde ser percebido com a loja em operação, e, apesar do Gestor

---

<sup>1</sup> B2C – Business to Consumer

de TI alertar periodicamente seus chefes sobre os possíveis problemas da loja, uma solução definitiva ainda não foi adotada.

Com uma demanda de negócio pela certificação ISO 27001, bem como a adoção de frameworks como o PCI, CoBIT e ITIL, a Direção se motivou a iniciar um processo de Gestão da Segurança da Informação, com a contratação de um CSO – *Chief Security Officer* para comandar esta mudança na empresa. Após conhecer o negócio e a estratégia da empresa, levantar requisitos legais e estudar casos compatíveis com o segmento do varejo eletrônico, o Security Officer levantou os processos da empresa, documentando-os através da notação BPMN. A Figura 1 ilustra o modelo do processo de pedido da Loja Virtual.

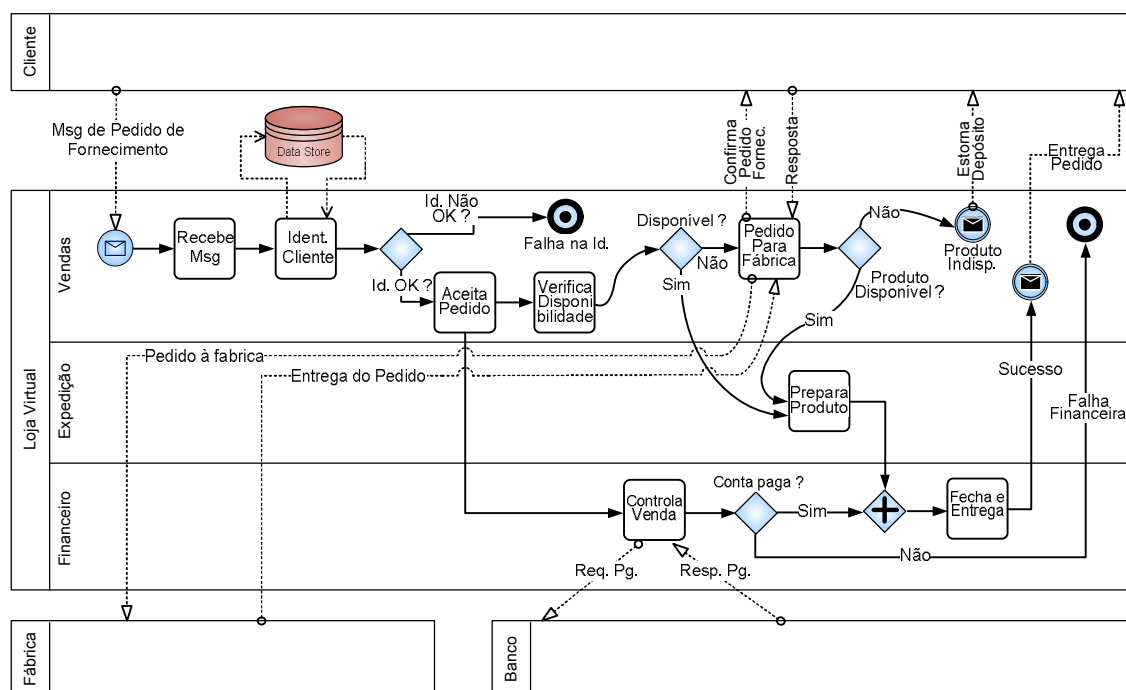


Figura 1 - Modelo em BPMN da Loja Virtual

De todos os possíveis processos onde o risco pode estar presente, será dado destaque ao processo de cadastramento de cliente, uma vez que, durante a entrevista, o Gestor de TI evidenciou o conhecimento de falhas existentes no código, que permitem ataques à loja virtual. A figura 2 ilustra o processo de solicitação de cadastramento. Nele, o cliente potencial envia um pedido ao administrador do sistema sobre o cadastro e recebe uma resposta sobre as demandas para este cadastro.

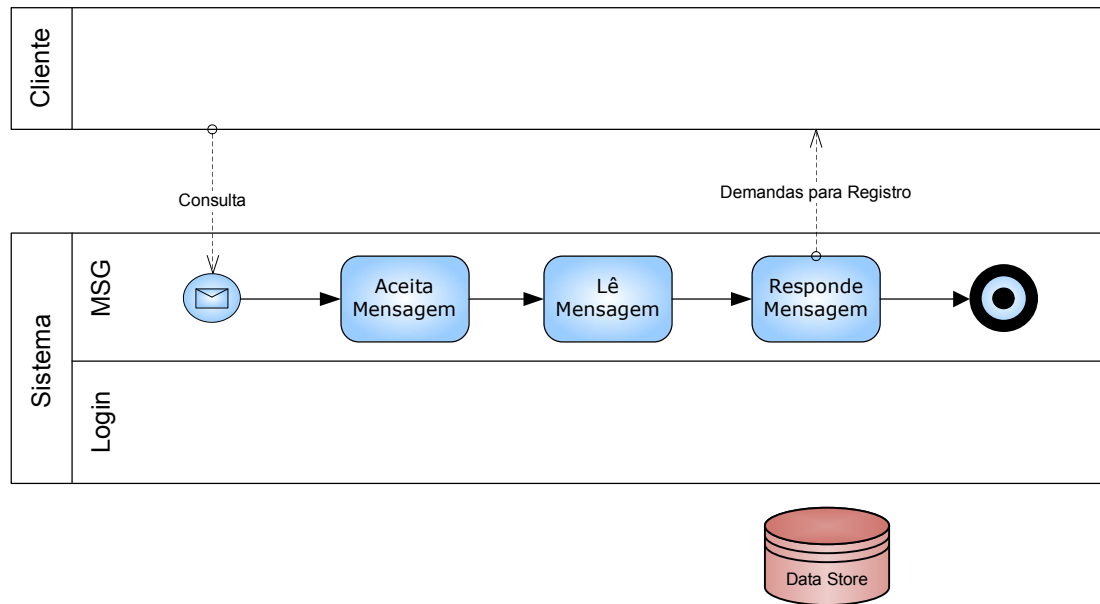


Figura 2 - Consulta para Pedido de Cadastro

Na figura 3 é ilustrado o processo de registro do cliente. Após receber as instruções (demandas para o registro), o cliente submete seus dados à loja virtual. O sistema aceita as informações para o registro, incluindo um login e uma senha, e inclui as informações em seu banco de dados.

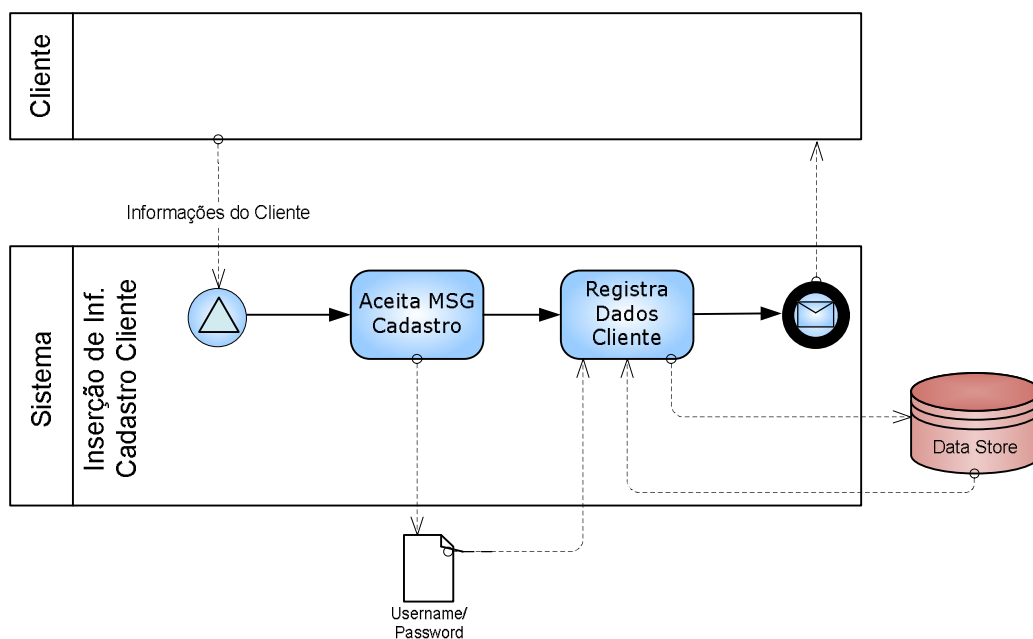


Figura 3 - Processo de Registro de Cliente

Após o cadastramento, o cliente estará apto a realizar pedidos de compra. Inicialmente, o sistema verifica a existência do login (username escolhido pelo cliente) e, logo a seguir, verifica a senha. Se as informações estão corretas, o usuário recebe o sinal de “sucesso” e está apto a usar o sistema para fazer pedidos, e se não estiverem, recebe um sinal de erro. A figura 4 ilustra este processo.

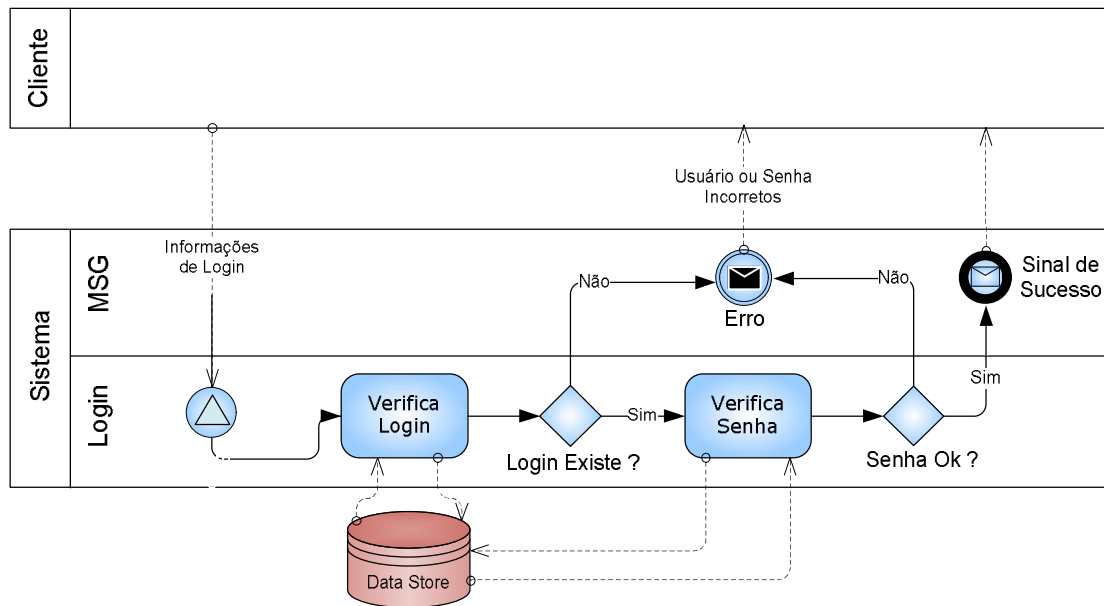


Figura 4 - Login no Sistema

Ao entrevistar o gestor do sistema, puderam ser evidenciadas questões óbvias. A combinação login / senha tem demandas de confidencialidade. Também há a demanda de Confiabilidade<sup>2</sup> do sistema como um todo, visando proteger o negócio. Uma situação de ataque está ilustrada na figura 5.

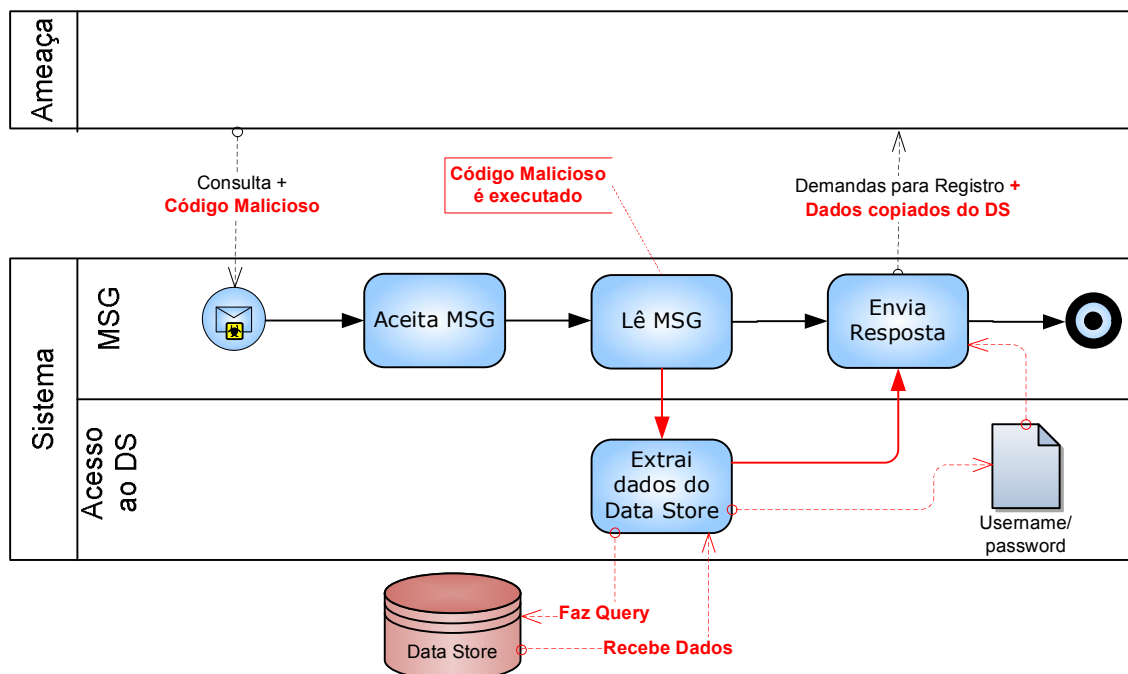


Figura 5 - Ataque ao Sistema

<sup>2</sup> Confiabilidade é um atributo adicional ao CID, que busca garantir que sistemas e processos funcionem da forma planejada.

Este possível ataque tem o potencial, segundo a observação especialista, de comprometer a confidencialidade de logins, senhas e com isso as demais informações cadastrais, como números de cartões de crédito e respectivos códigos de segurança de todos os usuários, possibilitando pedidos fraudulentos e comprometimento irreversível de imagem, com prejuízo crítico para a empresa. Há também o relato de situações ocorridas com outras empresas, como a PSN (Playstation Network), cujo comprometimento de informações dos seus clientes impactou a Sony em estimados 14 bilhões de yens (171 milhões de dólares), segundo a revista wired (<http://www.wired.com/gamelifelife/2011/05/sony-psn-hack-losses/>).

Faça sua proposta de solução com base nas informações disponíveis neste documento e arbitre o que for necessário. Considere que a empresa possui um sistema *no-break* de autonomia limitada, suficiente apenas para interrupções momentâneas de fornecimento de energia

Uma solução para este case será disponibilizada antes da prova no site <http://www.fredsauer.com.br>.

### **Anexo 1 – Base para extração dos critérios de aceitação de risco.**

Várias corporações já adotam, durante os estudos para a elaboração de seu planejamento estratégico, a prática da análise de riscos ao negócio. Instituições financeiras, por exemplo, por força da Instrução CVM nº 480 de 7 de dezembro de 2009, no seu anexo 24, realizam anualmente o “Formulário de Referência”, com a participação de auditores externos e membros de toda a empresa. As informações provêm da alta direção, que assume total responsabilidade pelas respostas ao formulário. No seu item 4 – FATORES DE RISCO, são evidenciadas situações que podem comprometer a saúde financeira da empresa, provocando perdas não apenas para a instituição como também para o investidor. Um exemplo completo deste formulário está disponível em <http://www.fredsauer.com.br>.

Seguindo a linha desta prática já existente no mercado, a empresa foco deste case identificou as seguintes situações de risco que devem ser tratadas no contexto do SGSI:

**Uma falha operacional pode provocar indisponibilidade da loja virtual, causando perdas nas vendas, ônus financeiros decorrentes da perda de receita, impactos aos parceiros e comprometimento da imagem.**

- Apesar da disponibilidade de recursos para manter a continuidade operacional da loja virtual, os mesmos são limitados e os sistemas e instalações operacionais podem parar de funcionar adequadamente por um tempo limitado, ficar temporariamente indisponíveis ou ainda totalmente fora de serviço devido a uma série de fatores, inclusive por eventos que estão inteira ou parcialmente fora de seu controle, dentre os quais: falta de energia e interrupção dos serviços de telecomunicações; quebras, falhas nos sistemas ou outros eventos que afetem terceiros como fornecedores ou prestadores de serviços; eventos causados por problemas locais ou de maior abrangência de natureza política ou social e ataques cibernéticos.
- Interrupções e falhas temporárias da infraestrutura física, do sistema operacionais ou da aplicação “loja virtual” que fornecem suporte aos negócios da corporação, ataques cibernéticos, ou divulgações não autorizadas de informações pessoais em seu poder, poderiam causar desgastes com o cliente, processos judiciais, multas regulatórias, sanções ou intervenção, reembolso ou outros custos de indenização e, por consequência, causar um efeito adverso sobre os resultados da corporação.

Por conta disso, a direção da empresa considera INADMISSÍVEL a aceitação deste risco, devendo o mesmo ser tratado.