

Ibmec Business School
Especialização em Segurança da Informação
IBMEC - Petrobras

**Disciplina: Tratamento de Incidentes de
Segurança**

Professor

Frederico Sauer, D.Sc.

fred@sauersecurity.com.br

Exercício: Elaboração de um GRIS e um PRI

Apresentação da Empresa-Alvo

Empresa para elaboração do GRIS e PRI

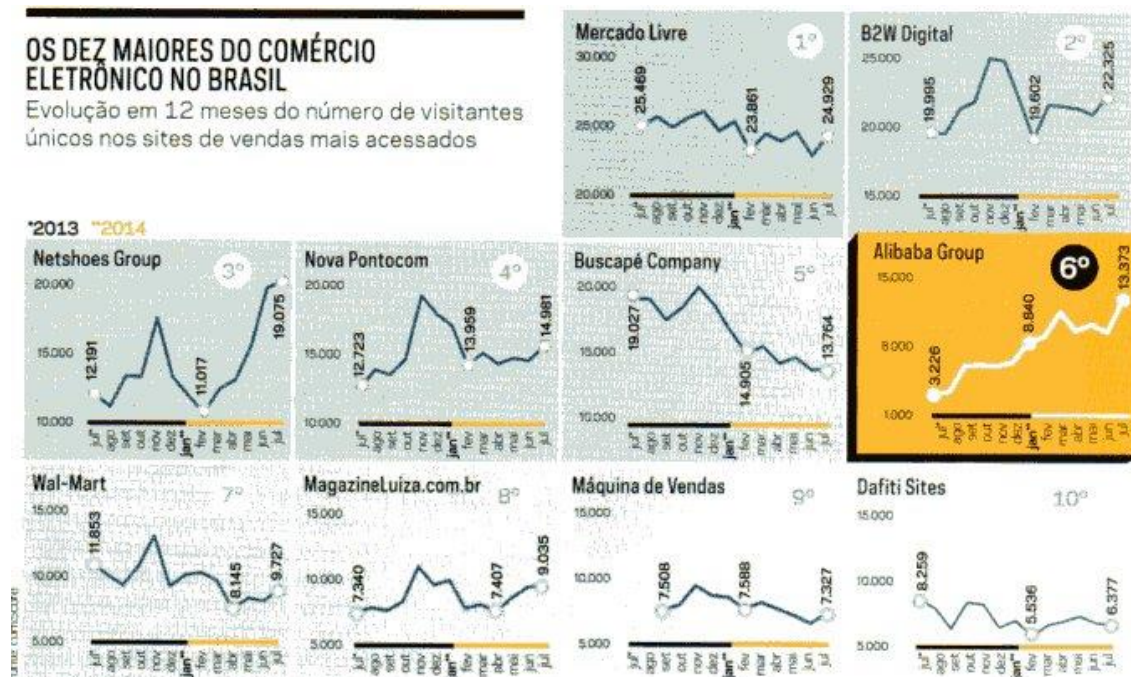
Este texto é a base dos exercícios a serem realizados durante a disciplina de Tratamento de Incidentes de Segurança da Informação. Os passos a serem realizados, e documentados nas folhas do final da apostila são:

- 1. Elaboração do primeiro esboço para criação de um GRIS; e**
- 2. Elaboração do primeiro esboço de um PRI para uma ameaça escolhida pelo grupo.**

O Case 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 durante o curso de Respostas a Incidentes de Segurança da Informação.

Como em inúmeras empresas atuais, os negócios de varejo realizados online possuem tendência de movimentação 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 B2C¹. O quadro 1, retirado da revista Carta Capital de outubro de 2014, nos mostra que o comércio eletrônico possui aumento significativo para empresas tradicionalmente físicas, como Walmart, Magazine Luiza e as empresas B2W, além de ser um excelente mercado para empresas exclusivamente virtuais, como a AliBaba e o Mercado Livre.

¹ B2C – Business to Consumer



Quadro 1 – Interesse de consumidores por opções no e-commerce entre 2013 - 2014

No caso da Loja Virtual deste exercício, a falta de planejamento, bem como ausência de envolvimento de todos os setores e principalmente falta de comprometimento dos especialistas em TI com a Segurança da Informação, provocou o lançamento de uma plataforma de vendas problemática, sujeita a ataques. A plataforma de compras online usa códigos antigos já prontos oferecidos pelo próprio ISP, que não foram devidamente testados quanto à segurança. Infelizmente, isso só pôde ser percebido com a loja em operação, e apesar do Gestor de TI alertar periodicamente seus chefes sobre os possíveis problemas futuros da loja, uma solução definitiva ainda não foi adotada (Típica falta da tríade: Tempo – Recursos – Pessoas).

Ocorre que, em virtude de incidentes de segurança da informação graves publicamente conhecidos, como os do Ingresso.com, LinkedIn, Sony e vários outros, surgiu uma nova demanda de negócio pela certificação ISO 27001:2013, bem como o interesse pela adoção de *frameworks* como o PCI, CoBIT e ITIL, e a Direção espontaneamente se motivou a iniciar um processo de Gestão da Segurança da Informação, iniciado com a contratação de um CSO – *Chief Security Officer* – para comandar esta mudança na empresa. Após tomar conhecimento do negócio e da estratégia da empresa, levantar requisitos legais e estudar casos compatíveis com o segmento do varejo eletrônico, o Security Officer mapeou os processos da empresa, documentando-os através da notação BPMN. A Figura 1 ilustra o modelo do processo de inserção de pedido no sistema da Loja Virtual.

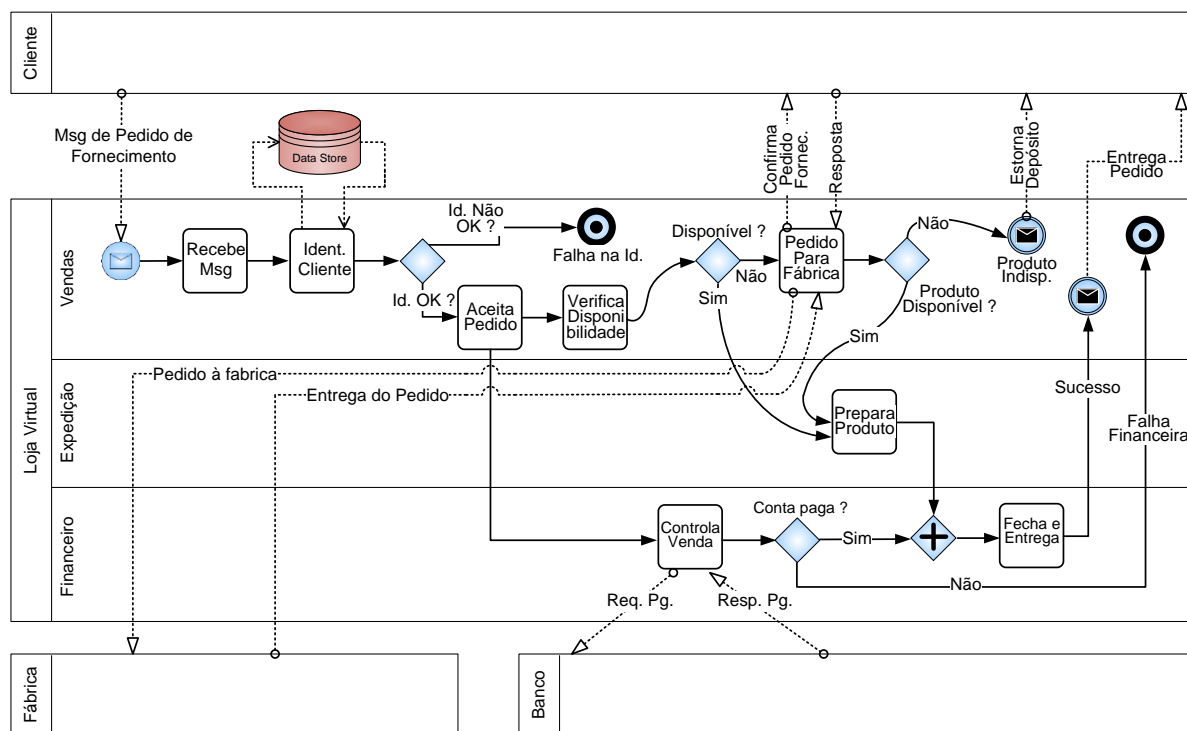


Figura 1 - Modelo em BPMN da Loja Virtual

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.

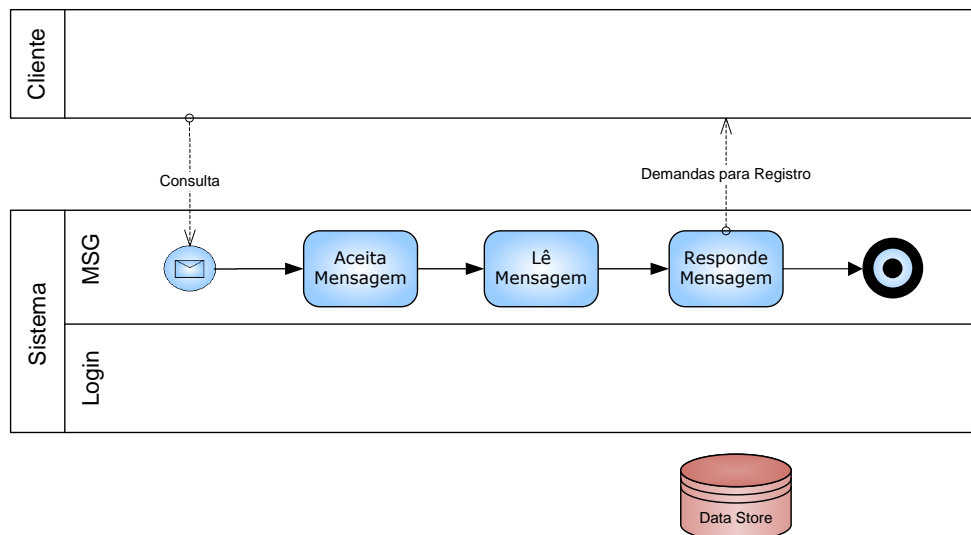


Figura 2 - Consulta para Pedido de Cadastro

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.

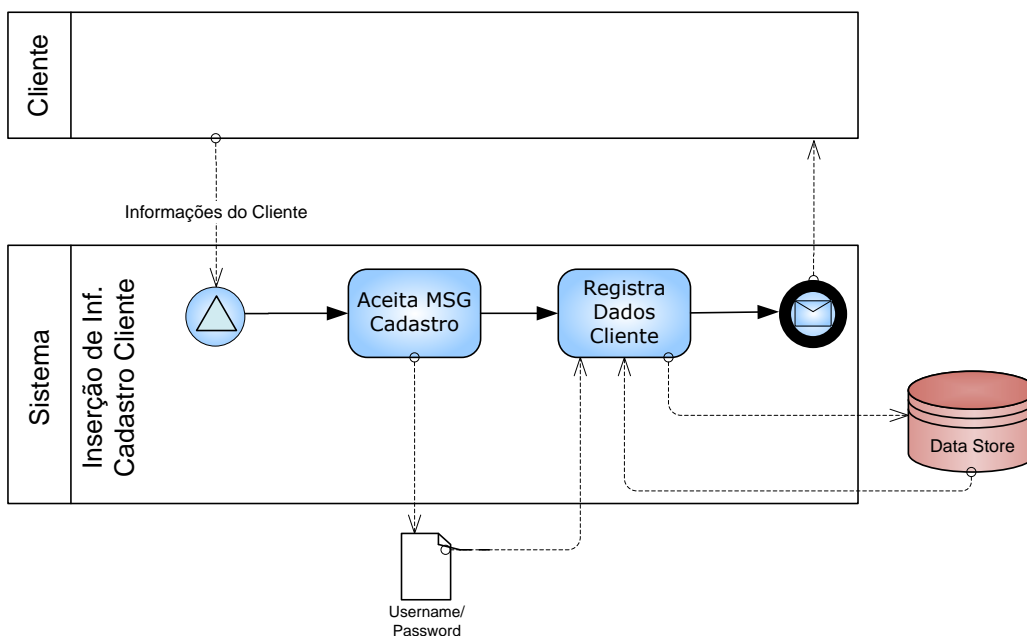


Figura 3 - Processo de Registro de Cliente

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.

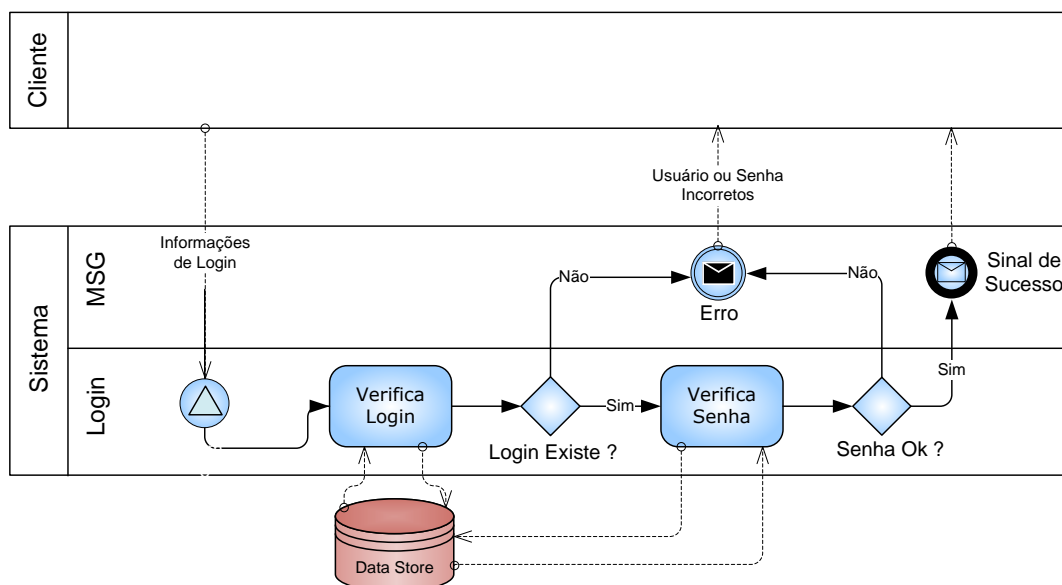


Figura 4 - Login no Sistema

Ao entrevistar o gestor do sistema, puderam ser evidenciadas questões óbvias. A combinação login / senha tem demandas de confidencialidade. Também há a demanda de Confiabilidade² do sistema como um todo, visando proteger o negócio. Uma situação de ataque está ilustrada na figura 5.

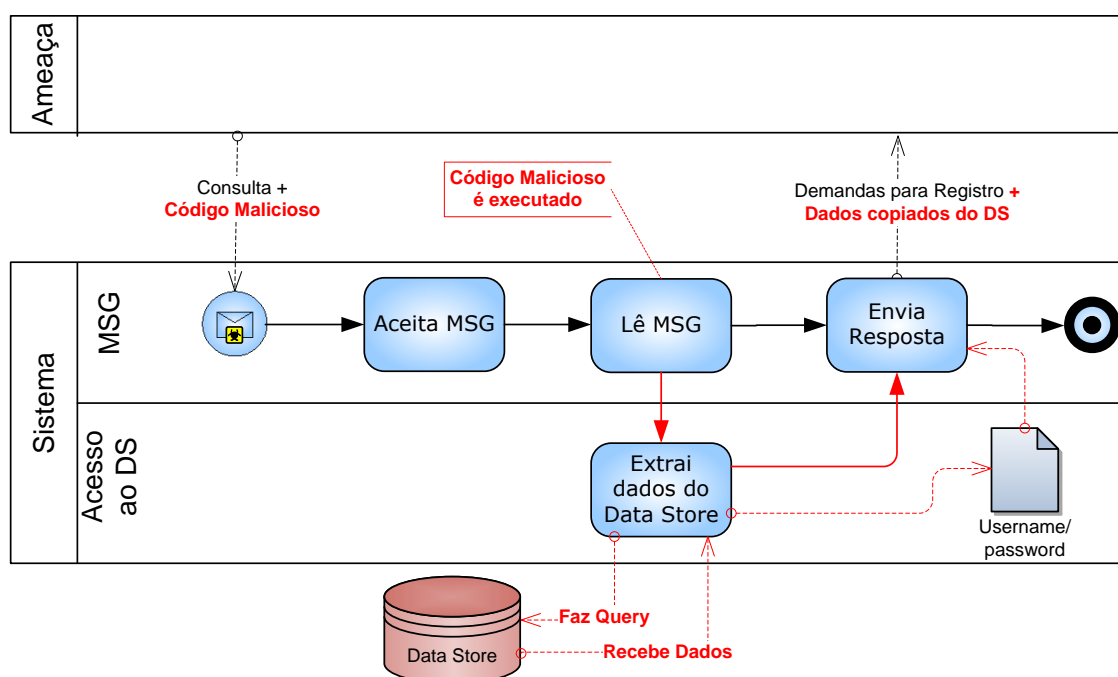


Figura 5 - Ataque ao Sistema

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

Este possível ataque, segundo a observação especialista, tem o potencial 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 possivelmente irreversível de imagem, com prejuízo crítico para a empresa. Há também o agravante 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/gamelife/2011/05/sony-psn-hack-losses/>).

O caso ilustrado é apenas um exemplo de vulnerabilidade descoberta cuja resolução deve ser priorizada, ao invés de se investir em contingenciamento, mas outras situações semelhantes podem ocorrer e o foco inicial das ações de resposta a incidentes deve levar esta experiência em consideração.

++++
Faça sua proposta de solução com base nas informações disponíveis neste documento e arbitre o que for necessário. Use os templates disponibilizados em <http://www.fredsauer.com.br> para seguir uma linha lógica durante o exercício. 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 –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 das ações do GRIS e do PRI:

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 de riscos decorrentes destes tipos de incidentes, devendo os mesmos serem tratados.