MBA EM GESTÃO EMPRESARIAL
FOCO EM TECNOLOGIA DE INFORMAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Prof. Dr.Frederico Sauer
fred@sauersecurity.com.br

Sauer, Frederico.

Gestão da Segurança da Informação, 1ª ed. Rio de Janeiro; UFF – LOGEMP- Cursos de educação continuada.
86 p.

Bibliografia

1. Segurança da Informação 2. Gestão I. Título

Coordenador
Prof. Martius Vicente Rodriguez y Rodriguez, DSc.
Email: martiusrodriguez@id.uff.br

Chefe de Departamento
Prof. César Ramos Barreto, DSc.

A sua opinião é muito importante para nós

Fale Conosco!
Central de Qualidade – UFF
✉ **mbalogemp@gmail.com**

Sumário

1. Programa da disciplina

1.1 Ementa

Conceito de Risco. A Informação como um ativo. Ciclo de Vida da Informação. Visão Corporativa (Vulnerabilidades e Ameaças). Retorno sobre o Investimento. Conceitos de Segurança. Equação do Risco. Papel do *Security Officer*. Plano Diretor de Segurança. Plano de Continuidade dos Negócios. Implementação de Controles de Segurança. Gestão de Risco.

1.2 Carga horária total: 16 horas/aula

1.3 Objetivos

- *Capacitar o aluno a enfrentar os desafios impostos pela mudança de paradigma nas empresas, planejando, gerenciando e implementando técnicas de Gestão de Riscos;*
- *Apresentar uma estratégia para integração das visões Técnica e de Negócios;*
- *Apresentar o conteúdo da ementa de uma forma gradativa e autocontida em exposições de soluções que usem as tecnologias a discutir; e*
- *Verificar requisitos básicos para a Gestão da Segurança da Informação nas empresas.*

1.4 Conteúdo programático

Gestão de Segurança da Informação	• A Informação como um Ativo • Visão Holística do Risco • Ciclo de Vida da Informação e os Desafios • Retorno do Investimento • Modelo de Gestão
Conceitos Básicos de	• Atributos da Informação

Segurança	• Perímetros de Segurança e Defesa em Camadas • Equação do Risco • Papel do *Security Officer*
Plano Diretor de Segurança	• Ciclo PDCA • Metodologia e Ferramentas para Geração do Plano
Plano de Continuidade dos Negócios	• Política de Segurança da Informação • Análise de Riscos e Vulnerabilidades • Implementação de Controles • Análise dos Impactos (*Business Impact Analysis*) • Estratégias de Contingência • Componentes do Plano de Continuidade

1.5 Metodologia

O conteúdo programático será apresentado através de slides, quando detalhes da vivência prática do professor serão comentados, estimulando a participação do aluno ao debate. Soluções padronizadas disponíveis serão associadas aos desafios da implementação da Gestão da Segurança da Informação nas empresas. Um Estudo de Caso abordando a metodologia proposta será realizado durante as aulas.

1.6 Critérios de avaliação

O grau total que pode ser atribuído ao aluno obedecerá a seguinte ponderação:

- ✓ 70% referente à avaliação individual, sob a forma de trabalho individual, a ser realizada após o término da disciplina.
- ✓ 30% trabalho realizado em sala de aula durante a apresentação do curso.

1.7 Bibliografia recomendada

SEMOLA, Marcos. **Gestão Estratégica da Segurança da Informação – Uma Visão Executiva**. 2ª edição. Rio de Janeiro: Editora Campus, 2014.

HUBBARD, W. Douglas. **How to Measure Anything – 3rd edition –** John Wiley & Sons, 2014.

ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — **Sistemas de Gestão da Segurança da Informação — Requisitos**

ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — **Código de Prática para Controles de Segurança da Informação**

ABNT NBR ISO/IEC 27003:2011 Tecnologia da informação – Técnicas de segurança – **Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação**

ABNT NBR ISO/IEC 27005:2011 Tecnologia da informação — Técnicas de segurança — **Gestão de Riscos de Segurança da Informação**

Curriculum resumido do professor

http://buscatextual.cnpq.br/buscatextual/visualizacv.do?id=C743786

Frederico Sauer Guimarães Oliveira é Doutor em Sistemas Computacionais (Tese em Gerencia de Redes) e Mestre em Ciências em Engenharia Elétrica (Dissertação em Segurança e Mobilidade na Internet) pela COPPE/Poli-UFRJ em 2007 e 1999, respectivamente. Auditor de Segurança da Informação Digital pela Marinha do Brasil de 1993 a 2010. Especialista em Análise de Sistemas e Engenheiro pela Universidade do Estado do Rio de Janeiro (UERJ). Graduado em 1986, atua desde 1987 na área de Tecnologia da Informação. É professor do FGV *Management* desde 1999 e docente em cursos de graduação e pós-graduação em TI. Coordenador e professor de cursos de Pós-graduação em Redes de Computadores e Segurança da Informação desde 2004. Autor de artigos em congressos na área de Segurança e Mobilidade em Redes. Exerceu a função de Security Officer da área de projetos estratégicos da Marinha durante 17 anos. Atualmente presta consultoria e dedica-se à área de ensino.

2. Slides comentados

A seguir, os slides usados na aula, juntamente com os principais comentários do professor, estão disponíveis para o aluno. Não há necessidade de registrar o que o professor está falando, tudo está documentado aqui. Procure apenas ouvir, questionar, interagir, de forma que tudo que está sendo ensinado possa ser completamente entendido por você.

Slide 1

MBA EM GESTÃO EMPRESARIAL

FOCO EM TECNOLOGIA DE INFORMAÇÃO

UNIVERSIDADE FEDERAL FLUMINENSE

Slide 2

O prof. Fred Sauer mantém um repositório de material no URL http://www.fredsauer.com.br

Slide 3

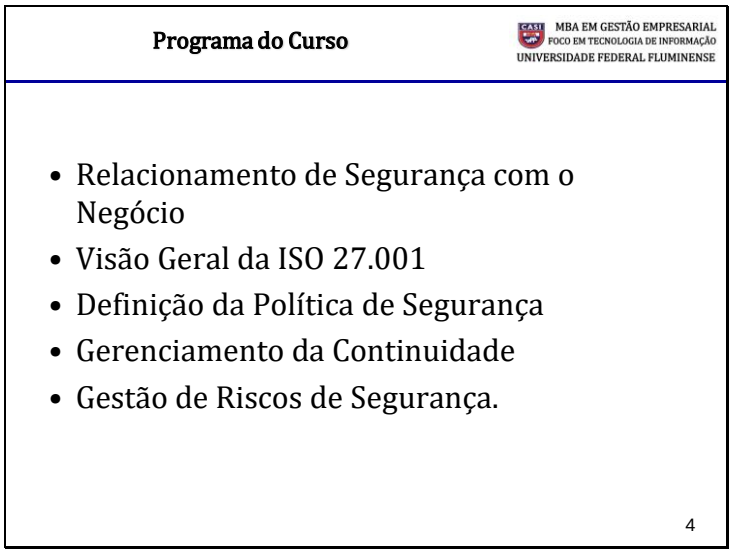
Preliminares

MBA EM GESTÃO EMPRESARIAL
FOCO EM TECNOLOGIA DE INFORMAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

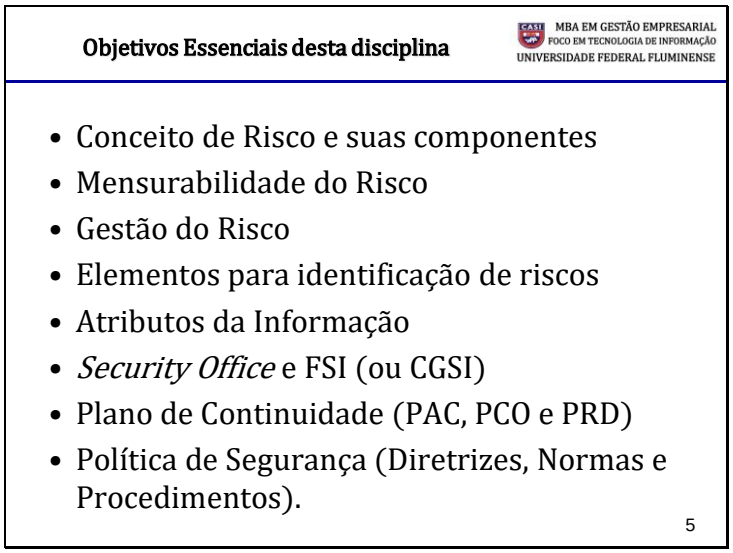
- Fred Sauer
  - Professor de MBA desde 1999
    - Redes de Computadores
    - Tecnologia Internet
    - Tecnologias Específicas e Emergentes
    - Gestão da Segurança da Informação
  - Security Officer da área de pesquisa estratégica da MB desde 1993
  - Membro da Comissão Permanente de Auditoria de SegInfo da MB desde 2001.

3

Slide 4


Programa do Curso
MBA EM GESTÃO EMPRESARIAL
FOCO EM TECNOLOGIA DE INFORMAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE
• Relacionamento de Segurança com o Negócio
• Visão Geral da ISO 27.001
• Definição da Política de Segurança
• Gerenciamento da Continuidade
• Gestão de Riscos de Segurança.
4

Slide 5



O curso seguirá uma linha processual, identificando inicialmente o conceito de Risco e como identificá-lo. Discutirá o maior desafio, que é a mensuração do mesmo. Enquanto variável probabilística, sua incerteza faz com que os empresários abdiquem de investimentos na proteção da informação sensível. A simples discussão em torno do tema já permite a redução das incertezas, possibilitando investimentos mais racionais e evolutivos, sem a adoção de soluções prontas e genéricas, tipicamente caras e de pouco ou nenhum retorno.

O Risco é dinâmico e acompanha as mudanças na empresa. Por isso, é mister a adoção de mecanismos de Gestão.

Riscos podem ser identificados através de suas componentes. Mas também são úteis outras fontes, como os incidentes já ocorridos e a experiência especialista, obtida dos gestores de processos de negócio.

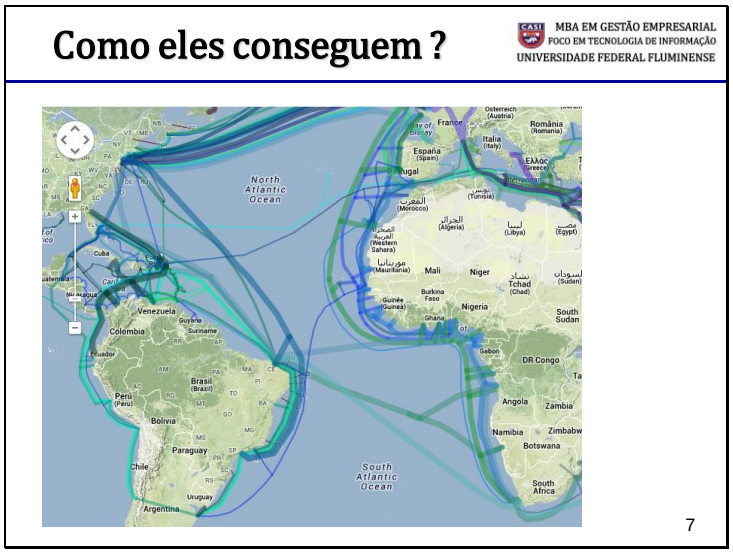
A Sensibilidade da Informação deve ser avaliada através de seus atributos. Neste curso será adotada a Análise CIDAL, que possibilita a avaliação dos principais requisitos da informação no que tange à sua demanda de proteções.

A demanda de uma estrutura para a Gestão de Risco, independente e atuante em TODOS os processos de negócio, responsável, por exemplo, pela existência de um programa contínuo de treinamento e conscientização, pode genericamente ser denominada de Security Office. O FSI, que nas normas é tratado como SGSI, possibilita a participação de todos, facilitando a criação da Cultura de SegInfo. O PCN e a Política de Segurança materializam os resultados da identificação de riscos, oferecendo Contingências (PCN) para os mais graves e Controles (PolSeg) para os demais.

Slide 6

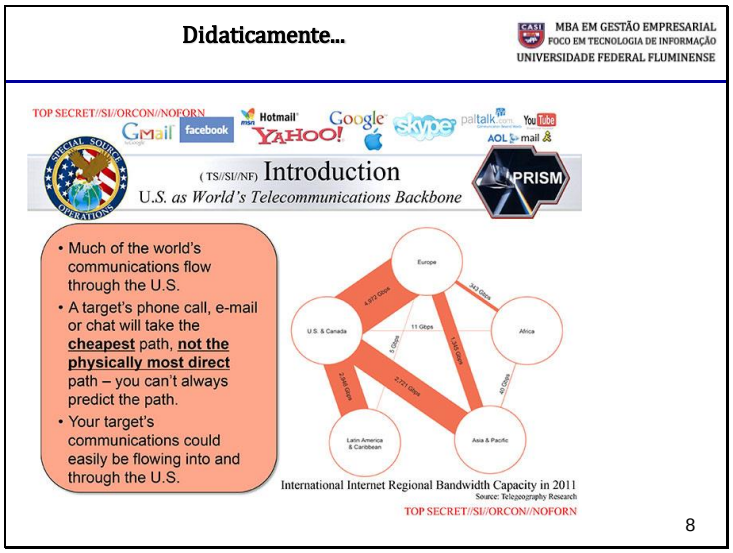
O momento atual é adequado para a motivação da direção para as necessidades no campo da Segurança da Informação. Os recentes incidentes evidenciaram a existência de procedimentos planejados com o objetivo de obter informações estratégicas importantes. Cabe aos gestores do negócio das empresas identificar seus ativos mais importantes, suas vulnerabilidades, e em função disso definir mecanismos que possam protegê-los de ameaças.

Slide 7



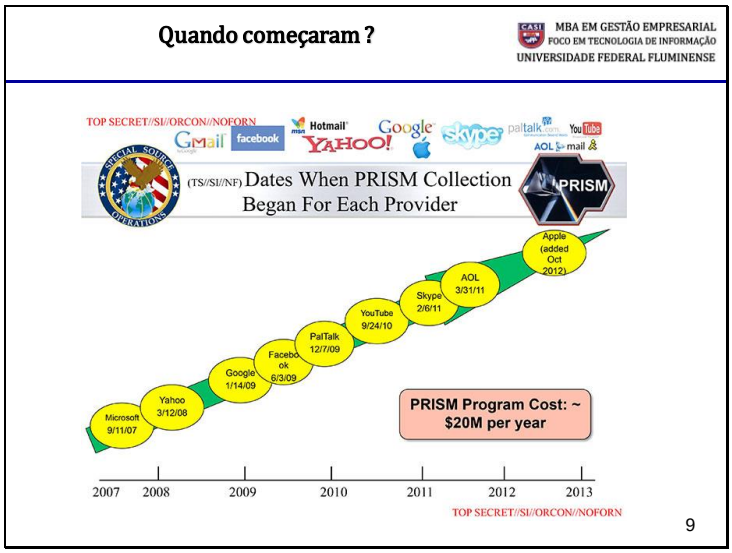
A figura ilustra os canais submarinos de fibras óticas, que implicam em passagem pelos Estados Unidos. Os maiores provedores de serviços de dados se encontram no hemisfério norte, possibilitando o acesso às informações.
Reativamente, o Brasil divulgou, após este escândalo, a existência de um projeto para construção de um cabo submarino para a Europa, já que o único disponível atual apenas suporta tráfego de voz.

Slide 8



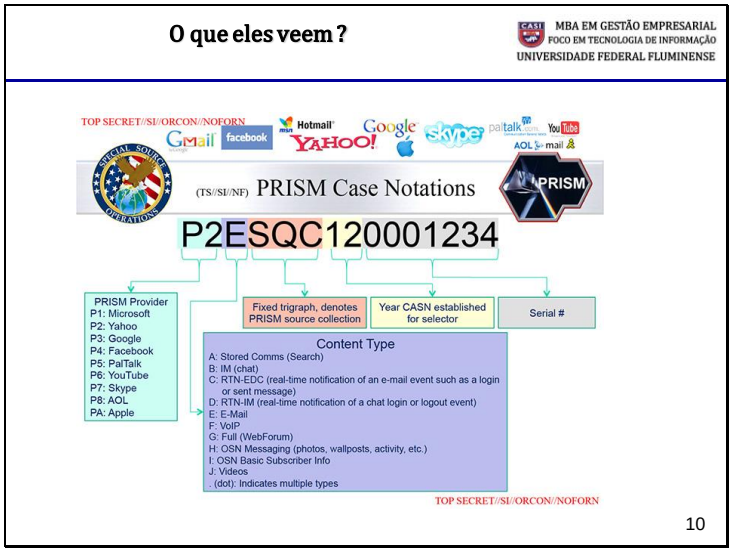
Este slide mostra o volume de tráfego entre os continentes. Praticamente não há tráfego direto entre a América Latina e outros lugares do mundo, sem passar pelos Estados Unidos.

Slide 9



Esta figura apresenta o cenário de evolução do PRISM. Segundo a figura, os grandes fornecedores de soluções para todo o mundo já estariam comprometidos com este projeto, inclusive a Microsoft (primeira a aderir) e a Apple (adesão recente). Entre eles, potências como o Google, Facebook, Skype e o Yahoo.

Slide 10



Os documentos são classificados no momento de sua obtenção, segundo um critério bem definido. Todo o material disponibilizado é bem elaborado e faz sentido. Observe que há classificação para email (AOL, Google, Yahoo) e VoIP (Skype). Nenhum tipo de comunicação estaria livre de interceptação pelo PRISM.

Slide 11

A falta de cultura de segurança, típica de uma sociedade que não convive com inimigos declarados, causa uma falsa sensação de segurança e o consequente despreparo para a adoção de medidas básicas de segurança. Foi tornado público que a Presidente da República teria recebido um aparelho telefônico com capacidade de criptografia, mas ela não usava. A Petrobras e a ANP, envolvidas com um dos maiores patrimônios naturais do país, admitiram não seguir internamente processos básicos de proteção à informação sensível, como por exemplo na contratação da Halliburton para o fornecimento de softwares e serviços para a avaliação do potencial dos campos petrolíferos brasileiros. A diretora da ANP chegou a declarar na época que um espião precisaria ser “paranormal” para obter informações sensíveis, uma vez que os bancos de dados são segregados da internet, mas não comenta o acesso de funcionários e serviços terceirizados em atividades sensíveis da Petrobras, bem como o uso interno de ferramentas públicas em trocas de *email* e outras formas de trafegar informação (gmail, google drive, dropbox, etc.).

Verdade ou não, NENHUMA empresa americana participou do leilão do campo de Libra, que acabou sendo leiloado pelo preço mínimo e foi adquirido pela própria Petrobras – 70%, pela Shell (Anglo-holandesa) e Total (francesa) – 20%, e empresas chinesas (10%).

Slide 12

A adoção de soluções pontuais, voltadas para a correção de falhas observadas apenas após incidentes é a mais frequente forma de tratar o risco. Tipicamente isso provoca maiores custos na solução, já que demanda urgência, além de não recuperar os danos à imagem e outros intangíveis.

Além disso, inevitavelmente grandes riscos poderão ser negligenciados, já que o foco destas ações é a correção de problemas, e não uma definição completa e planejada para Gestão dos Riscos em toda a corporação.

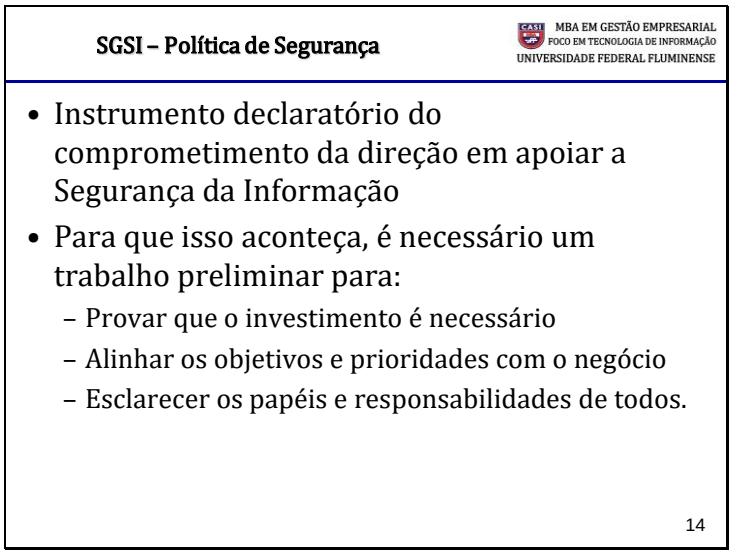
Slide 13

Um dos maiores desafios é a associação de Segurança com Negócio. O problema é o discurso diferente entre os especialistas de cada área. Cada gestor entende apenas do seu negócio e não tem facilidade de definir o nível de dependência que eles têm de outros processos. Imagine a seguinte situação: um gestor de TI precisa definir a autonomia do nobreak da empresa para o datacenter, e para isso ele precisa receber do negócio qual é o tempo mínimo de operacionalidade necessário para que processos importantes sejam concluídos ou direcionados para soluções contingentes. De uma forma geral, a resposta para esta pergunta é: não é admitida paralisação dos serviços de TI. Isso seria financeiramente inviável na maioria dos casos, por demandar um sistema completamente espelhado. É importante que cada gestor tenha uma visão holística, buscando compreender qual é a sua real necessidade em termos de operacionalidade mínima, definir ações contingenciais e interagir com os outros gestores para viabilizar esta solução. No caso ilustrado, o tempo mínimo ideal seria exatamente o tempo necessário para que o processo que depende dos insumos de TI possa se contingenciar.

A falta deste tipo de diálogo demanda mecanismos novos, baseados em medições e fatos, de forma a possibilitar o diálogo e a visualização de que riscos de Segurança da Informação são tão importantes quanto os demais riscos, que já são tratados (risco jurídico, operacional, etc.)

São também essenciais os mecanismos processuais distribuídos, já que, tradicionalmente a Segurança da Informação é vista dentro das empresas como uma disciplina pertinente apenas ao setor de Tecnologia da Informação. Os incidentes atuais mostraram que as ferramentas de TI para a Segurança existem e estão disponíveis, mas as pessoas e os processos não estão preparados para atuar de forma adequada à sensibilidade da informação e a sua importância para o negócio.

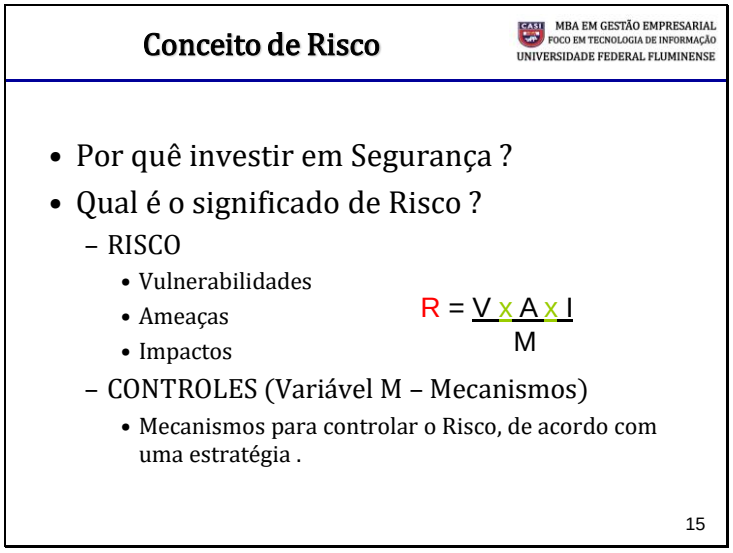
Slide 14



Uma das maiores dificuldades vislumbradas por todos que já atuam no cotidiano das empresas é: como fazer a direção perceber a importância de se investir em controle do risco em Segurança da Informação? Como obter prioridade com as limitações de recursos, principalmente em uma atividade onde o retorno do investimento não ocorre como lucro, e sim em evitar prejuízos? A resposta é simples. O primeiro passo na elaboração de um SGSI (Sistema de Gestão de Segurança da Informação) é obter a aprovação da Direção para o seu desenvolvimento, mediante justificativas claras e alinhamento com o negócio. Propondo ações compatíveis com o nível de risco e, principalmente, com os critérios de aceitação do risco definidos não por uma área técnica, e sim pelo negócio.

Neste contexto, o mais importante controle é a Política de Segurança, que envolve vários documentos que orientam e apoiam os processos de controle do nível de risco, de acordo com os requisitos do negócio e as leis e regulamentações relevantes. As diretrizes da Política são globais e abrangem não apenas todo o corpo de colaboradores da empresa como partes externas que, pela sua atividade, impliquem envolvimento em situações de risco. Assim, são criadas NORMAS para temas como o Controle do Acesso, a Classificação e Tratamento da Informação, a Segurança Física e do Ambiente e muitos outros, cobertos pela norma ISO 27002:2013. Estas políticas devem ser alvo de um programa de conscientização, educação e treinamento, de forma que todos as compreendam e as possam praticar. Para assegurar que as Políticas permaneçam pertinentes, adequadas e eficazes, devem ser planejadas análises críticas periódicas, bem como quando houverem mudanças no ambiente coberto pela Política.

Slide 15



A maior dificuldade para atingir-se os objetivos de Gestão do Risco é a obtenção dos recursos necessários para as ações de controle e as de contingenciamento. Os executivos baseiam-se em retorno do investimento na tomada de decisões, e não é simples a visão de que se deve investir conscientemente para também EVITAR prejuízos. Convém também elucidar as pardas intangíveis, como os comprometimentos da imagem da corporação, com a natural perda de oportunidades, como fatores impactantes.

A decisão pela gestão consciente e planejada da SIEMENS – ilustrada no caso disponível no repositório do professor – que investiu durante dois anos maciçamente na formação de cultura de segurança através de um código de ética. Demitiu os funcionários que não se alinharam, inclusive o presidente da SIEMENS Brasil, sob suspeita de desvio de recursos. Em virtude disso, a empresa obteve o índice mais alto possível no quesito "sustainability", onde o compromisso com a ética está inserido, na bolsa de Dow Jones.

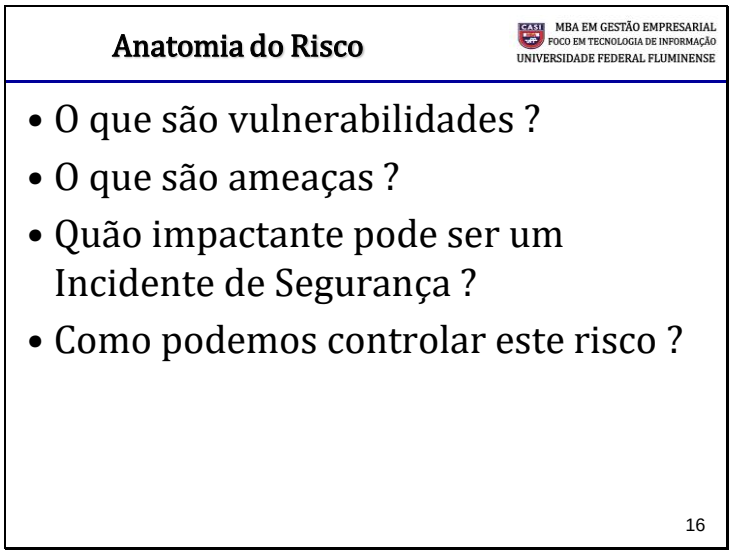
O Risco não é uma variável absoluta, e sim derivada da combinação de outras 4:

A **Vulnerabilidade** é um elemento PASSIVO, pertencente ao contexto da empresa e que pode ser identificado, mensurado e administrado.

As **Ameaças** são ATIVAS, porque exploram vulnerabilidades causando impactos. Sem vulnerabilidades a ameaça não se locupleta, e a pura e simples existência de vulnerabilidades não implica necessariamente em impactos, já que as vulnerabilidades são passivas e apenas possibilitam impactos na presença de ameaças.

Os **Impactos** são as consequências, tangíveis e intangíveis, da exploração de uma ou mais vulnerabilidades por ameaças. Sua mensuração é essencial para o sucesso da Gestão de Riscos, já que os **CONTROLES** (M) devem ser proporcionais aos impactos para o negócio decorrentes de um incidente de segurança. O RISCO deve ser analisado em relação às estratégias e a natureza do próprio negócio.

Slide 16



Resumindo, as VULNERABILIDADES são condições favoráveis para a ocorrência de incidentes, como o descumprimento de requisitos legais, treinamento inadequado, operação fora das condições consideradas seguras, etc. São facilmente visíveis e mensuráveis. As AMEAÇAS são elementos ATIVOS, intencionais ou não, que exploram VULNERABILIDADES causando IMPACTOS. Podem ser de natureza FÍSICA, TECNOLÓGICA ou HUMANA, assim como as vulnerabilidades. É típico colocar-se de lado a preocupação com riscos sob o argumento que as demandas do negócio são mais importantes que a operação segura. No entanto, a história tem mostrado que os incidentes de segurança têm comprometido a solidez de empresas aparentemente inabaláveis, como a LOCAWEB, que tinha a melhor estrutura disponível na época do "*co-location*", mas a disseminação de reclamações através das redes sociais (veja http://loukaweb.com) causou a migração de clientes, bem como a perda de novos clientes para outros fornecedores de serviços de nuvem, gerando uma concorrência que antes era pequena. Talvez esta situação seja reversível com o tempo, mas ela poderia ter sido evitada com uma política de Gestão de Riscos de Segurança da Informação, uma vez que a imagem é a mais importante informação agregada a uma empresa.

Riscos podem ser controlados através de Políticas de Segurança, onde se busca evitar que incidentes aconteçam, e uma sólida e atuante Gestão de Riscos, para que as mudanças do nível do risco possam ser percebidas e tratadas a tempo.

Slide 17

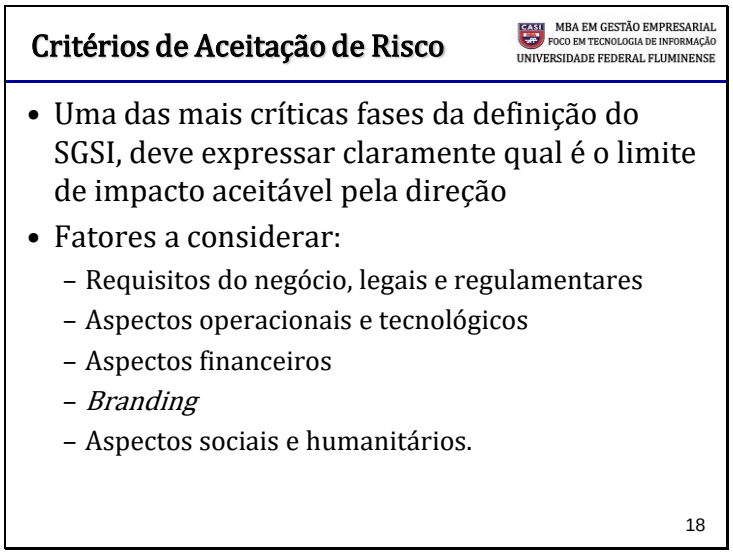
Este é o grande desafio do risco. O nível de risco é dinâmico em função das mudanças no ambiente. O nível aceitável de risco é uma decisão exclusiva da direção, com base em requisitos e expectativas do negócio, e não é trivial a sua definição. Se ele é aceito apenas em nível muito baixo, o custo com a gestão do risco será muito alto e talvez comprometa o desempenho produtivo da empresa. Por outro lado, se ele é assumido e se admite a operação com alto nível de risco, os gastos serão baixos e a produtividade será pouco ou nada afetada, mas as chances de ocorrer incidentes serão muito maiores.

O objetivo é, com o passar do tempo e a melhor compreensão dos desafios, a escolha de um nível aceitável de risco que seja exatamente o limite entre a existência de eventos de segurança que são controlados por regras de Política de Segurança (obviamente, que todos conheçam e sejam capazes de cumprir), e Incidentes de Segurança, para os quais apenas ações de contingenciamento resolvem. Isso é Gestão de Risco.

Em termos práticos, esta figura mostra que, ao identificar situações de risco envolvendo eventos de segurança, devemos definir políticas para trata-los, e para incidentes, **além** das políticas são necessárias ações para o contingenciamento do negócio.

Obs.: **Evento de Segurança** é uma ocorrência que indica uma possível violação da Política de segurança ou falha de controles, ou ainda uma situação desconhecida, que possa ser relevante para a segurança da informação. **Incidente de Segurança** é um ou uma série de eventos indesejados ou inesperados com grande probabilidade de comprometer o negócio e ameaçar a segurança da informação. O uso de uma *pendrive* contaminada com vírus em uma máquina da empresa, cujo vírus é limpo no momento de sua inserção na USB é um evento. Se o vírus não fosse identificado e contaminasse a rede, impactando a prestação de serviços de conectividade, seria um incidente.

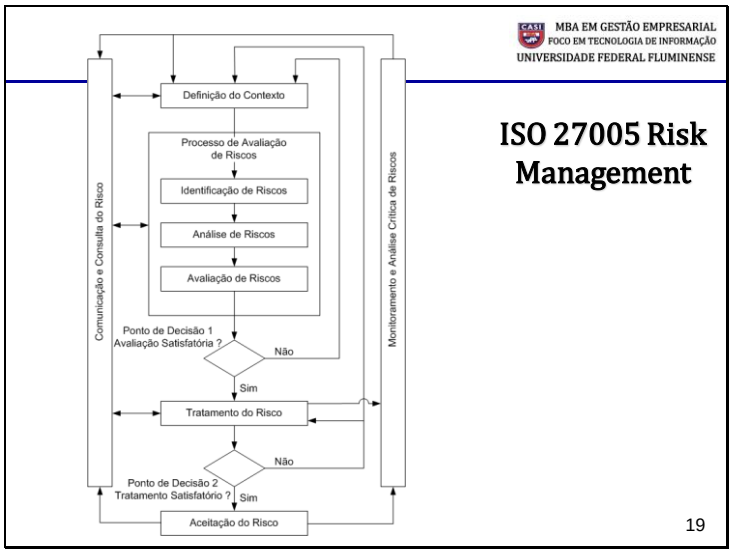
Slide 18



Caso esta fase não seja feita de forma razoável, teremos dois possíveis extremos indesejáveis: ou o nível de risco aceitável é demasiadamente baixo e o investimento em controles será muito alto, ou o inverso, onde o nível aceitável estipulado é alto e, apesar do baixo custo das soluções, a empresa corre sério risco de impactos irreversíveis e/ou irrecuperáveis em caso de incidente. O ideal é encontrar o equilíbrio, o que só é possível com o envolvimento de todos os gestores, de forma que o real nível de risco e as suas soluções de controle sejam adequadas ao negócio.

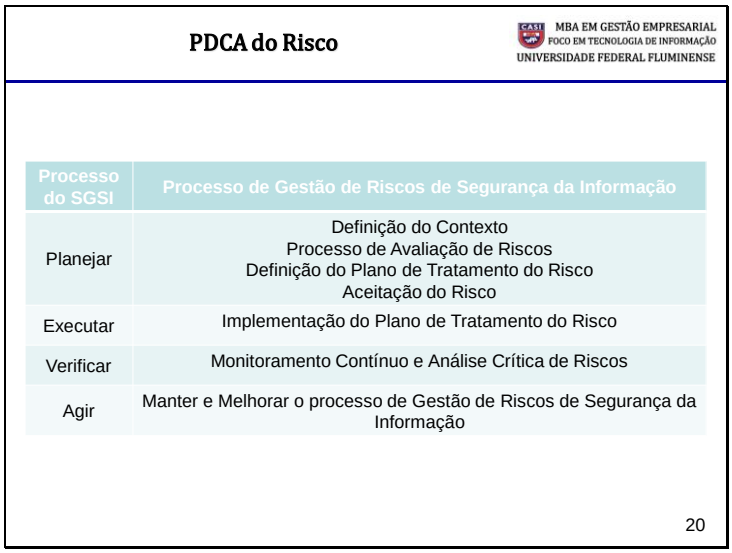
Cada empresa terá uma realidade diferente a considerar, mas de um modo geral, Requisitos do negócio da empresa, que envolvem a manutenção do *market share*, são essenciais. Por sua vez, requisitos legais e regulamentares, como o cumprimento de contratos e não descumprimento das leis vigentes, é obrigatório de ser considerado. Alguns aspectos operacionais e tecnológicos relacionados com a produtividade da empresa são importantes. A manutenção e fortalecimento da marca (*Brand*) é relevante. Em determinados momentos, questões sociais e humanitárias também devem ser levadas em consideração.

Slide 19



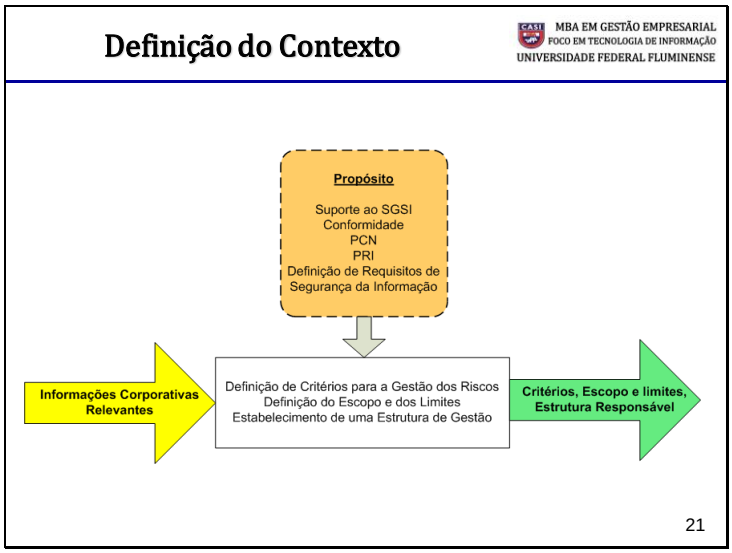
O enfoque interativo permite minimizar o tempo e o esforço despendidos na identificação de controles necessários e, além disso, possibilita que riscos de alto impacto ou de alta probabilidade possam ser adequadamente percebidos e avaliados.
A revisão do contexto é uma nova análise dos critérios de avaliação de riscos, de aceitação de risco ou de impacto, possivelmente em partes limitadas do escopo.
É interessante ressaltar a importância da comunicação do risco às partes interessadas, existente em todas as fases.
A avaliação do risco é a comparação objetiva dos riscos evidenciados e estimados (em sua criticidade) com os critérios de aceitação de risco definidos pela direção.

Slide 20



O ciclo PDCA da Gestão do Risco é semelhante ao do SGSI. Na fase PLAN são obtidos os insumos e elaborados todos os planos e estratégias para controlar o risco, até a aceitação dos riscos residuais. O resto é idêntico. Por conta disso, sugere-se a adoção do PDCA modificado, que será apresentado mais adiante, onde o início do trabalho é o monitoramento do ambiente, a criação da cultura corporativa de segurança e o desenvolvimento do hábito de registrar e notificar eventos e incidentes, criar a estrutura e iniciar discussões abertas e claras ANTES de se criar regras e investir em ferramentas.

Slide 21

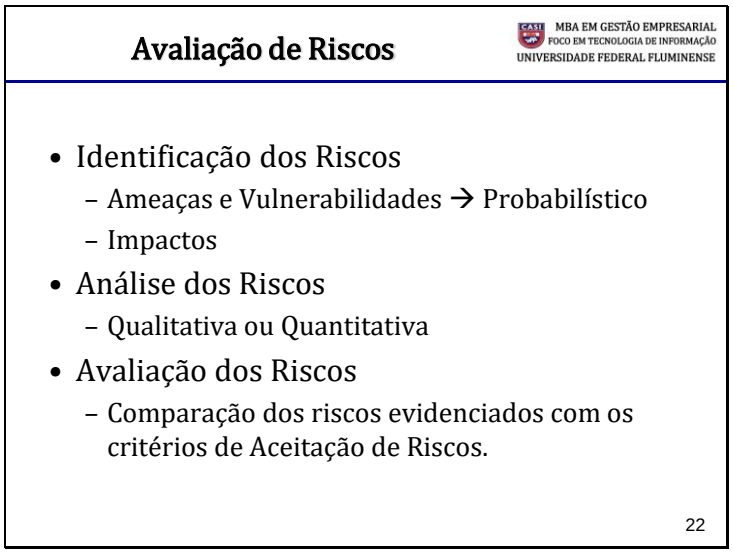


Definir o contexto significa estabelecer os critérios básicos necessários para a Gestão de Riscos da Segurança da Informação, definir o escopo e os limites, além de uma organização apropriada para a Gestão de Riscos. A definição do contexto é importante porque os propósitos da Gestão de Risco podem variar de acordo com suas motivações. Ele pode se destinar apenas a suportar um SGSI, mas também pode ser um instrumento de *compliance*, servir como instrumento de preparação de Planos de contingência e Planos de Resposta a Incidentes ou até servir como instrumento para descrição de requisitos de segurança para um produto ou serviço.

O escopo também é decisivo nesse processo, porque nele se estabelecem os objetivos estratégicos da organização, os processos envolvidos, requisitos legais e regulatórios, informações sobre o ambiente a ser gerenciado e suas interfaces com outros ambientes. Um escopo pode ser uma aplicação de TI, toda a infra de TI, um processo de negócio específico ou uma parte da organização.

A definição dos critérios de avaliação e aceitação de riscos também é feita nessa fase. Para a avaliação, devem ser usados como balizadores o valor estratégico dos processos, a criticidade dos ativos e da informação, os requisitos legais e regulatórios e as expectativas das partes interessadas. Os possíveis impactos envolvem comprometimento da informação sensível, operações de negócio comprometidas, perda de oportunidades e danos à imagem, por exemplo. Para a aceitação, deve ser definida uma escala envolvendo fatores financeiros, operacionais e intangíveis.

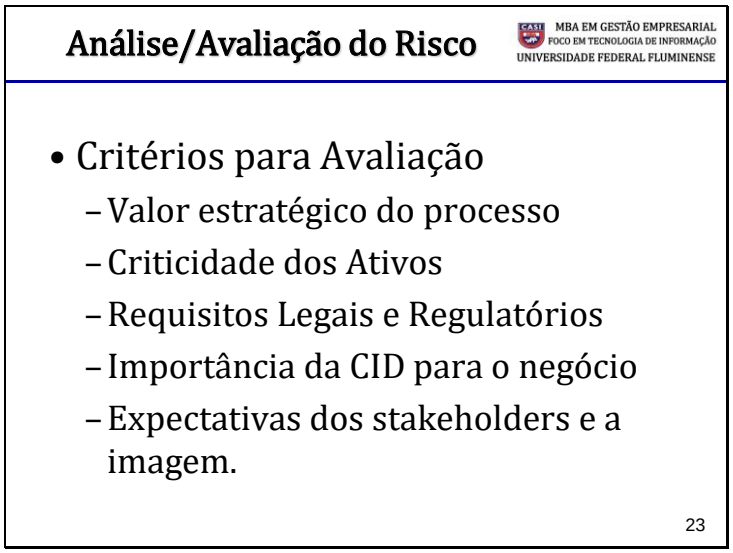
Slide 22



O processo de avaliação de riscos é técnico, logo, pode ser aprendido sem dificuldade pelos gestores. Com base no escopo definido, cada gestor deve quantificar ou descrever qualitativamente os riscos evidenciados de forma priorizada, conforme os critérios estabelecidos. Após determinar o valor dos ativos, o gestor identifica as vulnerabilidades existentes e as possíveis ameaças, identifica os controles já existentes e o seu efeito no risco determina as consequências da ação da ameaça e prioriza os riscos de acordo com os critérios estabelecidos durante a definição do contexto.

As ameaças podem ser elencadas a partir da análise de eventos e incidentes de segurança ocorridos na própria empresa ou empresas semelhantes, além da experiência especialista dos gestores, conforme já comentado. Elas podem ser naturais ou humanas, acidentais ou intencionais. Elas podem surgir de fora ou de dentro da própria organização. Deve-se realizar um esforço na obtenção de probabilidades realísticas da ocorrência de ameaças no ambiente, em função da importância desta percepção na priorização dos riscos e a determinação de investimentos na sua contenção e contingenciamento. As vulnerabilidades são mais fáceis de serem identificadas a partir de listas de boas práticas (como a ISO 27002:2013) que não são cumpridas. Os impactos, conforme já dito, podem contabilizar tempo perdido em recuperação, custo com a contratação de especialistas para reversão da situação de crise, perda de clientes atuais e futuros e comprometimento de imagem, por exemplo.

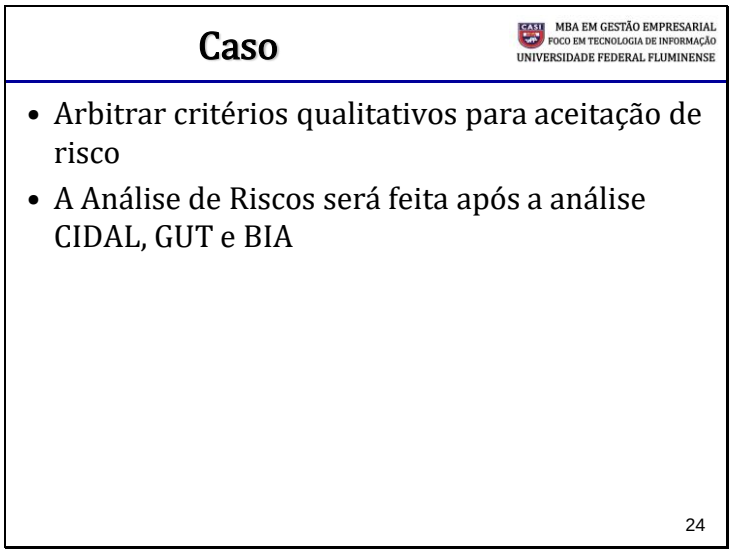
Slide 23



Critérios já comentados anteriormente. São as entradas do processo de Análise e Avaliação de Riscos.

A análise de Riscos pode ser quantitativa ou qualitativa, ou ainda uma combinação de ambas. Na prática, a análise qualitativa é usada inicialmente, porque o processo é menos complexo e menos oneroso. Nela são usados atributos qualificadores que descrevem a magnitude das consequências potenciais, de forma que facilite a compreensão e a identificação pelos envolvidos. Devem ser usadas escalas diferentes para riscos diferentes. Na análise quantitativa a escala usa valores numéricos, tanto para os impactos (consequências) como as probabilidades de ocorrência (Vulnerabilidades x Ameaças). Para uma avaliação realística, há grande dependência de uma consistente amostra de dados históricos da própria empresa para a obtenção de valores de probabilidades de ocorrência e de prejuízos. Convém que a incerteza sobre estas informações seja considerada durante a análise, com o objetivo de evitar investimentos incompatíveis com os reais riscos.

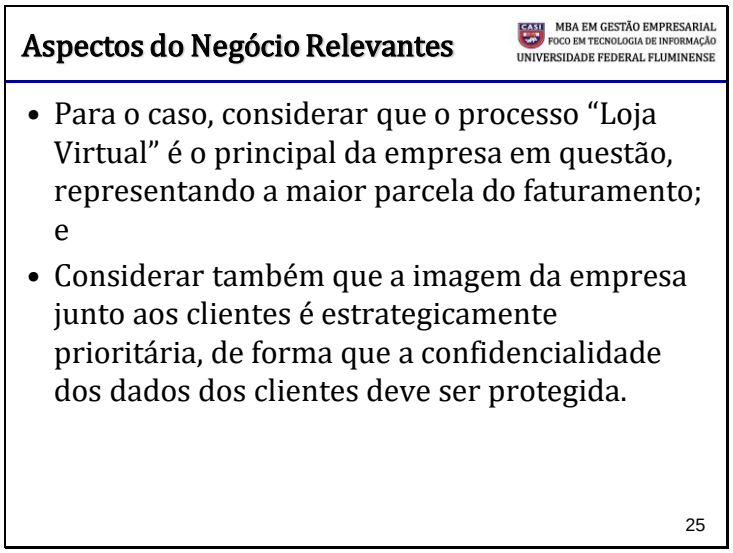
Slide 24



Com base no texto fornecido no final da apostila e no seu anexo – FATORES DE RISCO – identifique os critérios para aceitação do risco e os documente no template, para o processo de avaliação que será feito mais adiante.
O caso é baseado no artigo "*Towards Definition of Secure Business Process*", de Olga Altuhhova, Raimundas Matulevičius e Naved Ahmed, publicado em 2012 no livro Advanced Information Systems Engineering Workshops (pg. 1-15), da editora Springer Berlin Heidelberg. Nele, o BPMN (Business Process Modelling Notation) é usado na Gestão de Riscos. Vamos fazer o Estudo de Caso em fases:

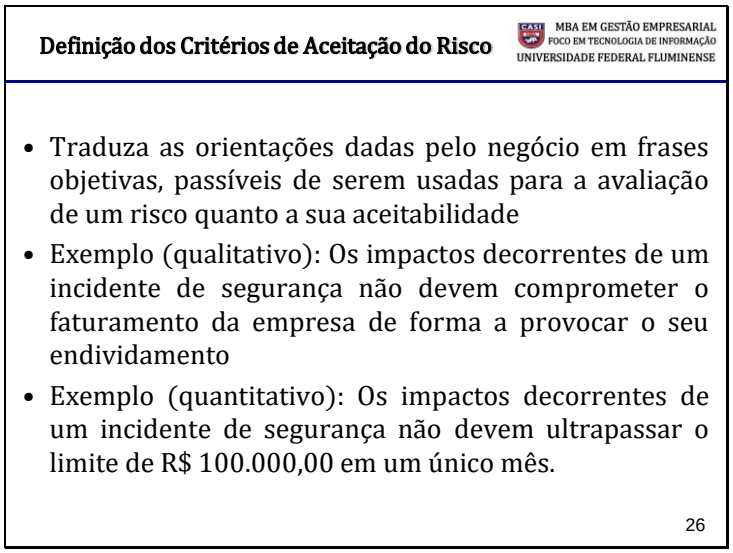
- Definição de Critérios de Aceitação do Risco, com base nas informações do texto;
- Mapeamento dos Riscos no Processo ilustrado no Caso;
    - Listando ativos do risco;
    - Identificando vulnerabilidades nos ativos e possíveis ameaças capazes de explorar as vulnerabilidades evidenciadas;
    - Análise de Riscos com CIDAL e GUT e BIA.
- Avaliação dos Riscos - Comparar resultados com os Critérios de Aceitação do Risco
- Propor ações de Política de Segurança e de Continuidade dos Negócios onde cabível, de acordo com as estratégias de tratamento do Risco: Modificar; Reter; Evitar ou Compartilhar. Também é possível combinar as ações.

Slide 25



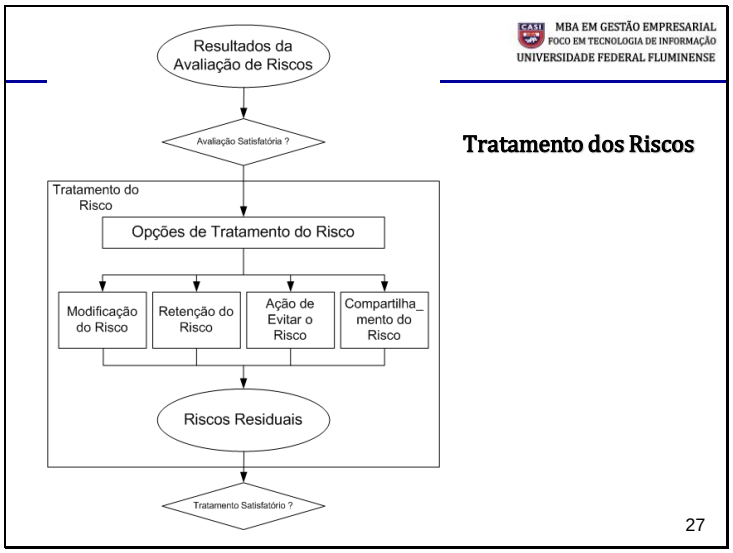
Definir as prioridades do negócio é um importante passo para direcionar as ações de Gestão da Segurança da Informação.

Slide 26



De uma forma geral, as empresas não possuem a cultura de registrar as lições aprendidas de forma quantitativa. Isso dificulta a tarefa de decidir se um determinado risco é aceitável ou não, além de tornar a tarefa de definir um valor para investir na contenção do risco e seu eventual contingenciamento de impactos. Caberá a equipe de gestão a definição de mecanismos para o registro destas informações e a sua transformação em indicadores a serem usados na tomada de decisão.
Uma boa abordagem é iniciar o trabalho de forma qualitativa e evoluir para a quantitativa aos poucos.

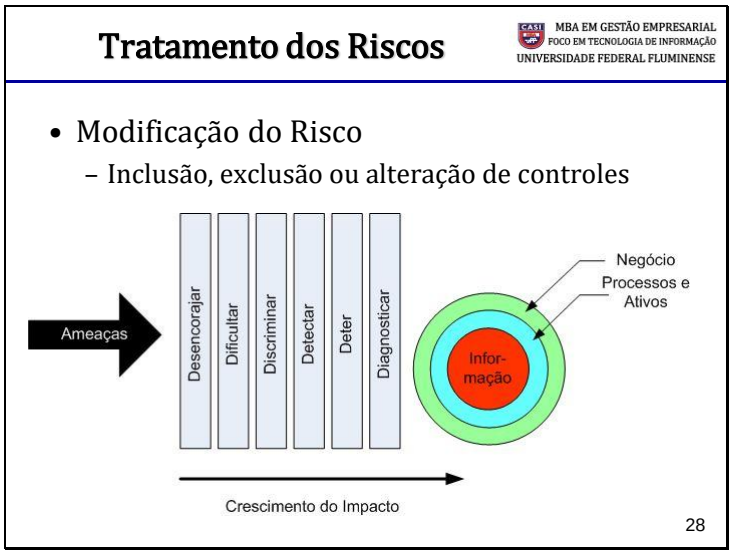
Slide 27



O tratamento de Risco é a etapa que segue a avaliação do risco. Nela, em função da identificação e mensuração de riscos feita na etapa anterior, podem ser adotadas quatro estratégias, conforme orientação da ISO 27005: 2011:

- **Modificação do Risco** –Nesta estratégia busca-se alterar o nível de risco através da inclusão, exclusão ou alteração de controles. A forma mais comum de modificação é a mitigação, através da inserção de controles para reduzir o risco, mas é importante prever a possibilidade, por exemplo, do relaxamento de controles pela redução da probabilidade de ocorrência como, por exemplo, a redução do tamanho de uma senha ou a periodicidade de sua troca, em virtude da percepção do amadurecimento da cultura de segurança dos colaboradores.
- **Retenção do Risco** – Quando o nível de risco é aceitável, não há necessidade de implementar controles adicionais porque os atuais são satisfatórios. Neste caso, basta a consciência de sua existência e a manutenção do monitoramento para evitar que o mesmo seja aumentado e ultrapasse os limites aceitáveis sem a ciência dos envolvidos;
- **Ação de Evitar o Risco** – Evitar a atividade que dá origem a um determinado risco. Esta estratégia é usada quando os riscos são muito altos e os custos de um tratamento de modificação é proibitivo para a empresa. Neste caso, a solução é modificar as condições que uma atividade ou parte dela ocorre, como por exemplo mudando um datacenter de lugar quando há grande probabilidade de inundação.
- **Compartilhamento do Risco** – Quando há outras entidades que possuem maior capacidade para gerenciar o risco. É importante observar que o compartilhamento cria novos riscos e pode modificar riscos existentes, demandando uma nova análise de riscos após a decisão pelo seu compartilhamento. Pode ser, por exemplo, feito através de seguro para eventuais prejuízos ou a subcontratação de um terceiro com expertise na gerência do risco identificado. É bom lembrar que não é possível compartilhar responsabilidade legal por impactos.

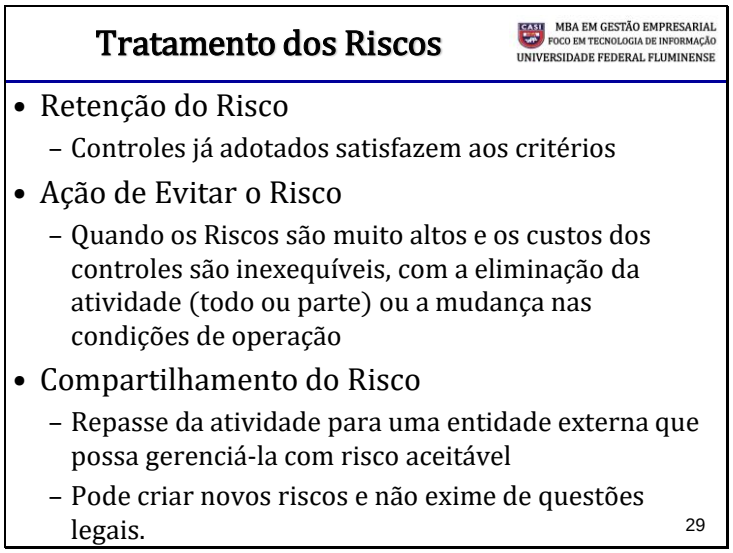
Slide 28



O processo de criação de controles deve, por questões de racionalização de recursos e maior facilidade de implementação e monitoramento, ser realizado em camadas, onde quanto mais a ameaça se aproxima dos ativos (e suas vulnerabilidades), mais especializada é a proteção.

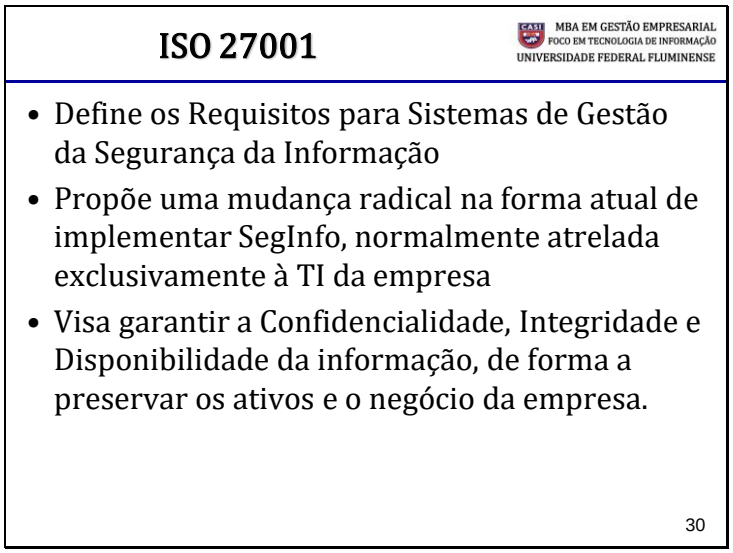
Na camada de "**Desencorajar**", se usa a própria política, avisos, alarmes e tudo que possa desestimular uma ameaça em iniciar um ataque. Estatísticas disponíveis mostram que esta barreira é bastante eficaz, principalmente quando a ameaça não está fortemente determinada a causar impactos. A barreira de "**Dificultar**" impõe uma eliminação de interfaces diretas entre o ativo e seus possíveis elementos ameaçadores. A burocratização de procedimentos e a imposição de restrições físicas de acesso é um exemplo. A barreira de "**Discriminar**" é a definição de restrições de acesso com base na necessidade de conhecer. A barreira da "**Detectar**" oferece um recurso para identificar uma ameaça que tenha sido bem-sucedida na superação das barreiras anteriores, e a barreira de "**Deter**" visa proteger o ativo bloqueando o acesso a ele pela ameaça que superou todas as proteções anteriores. Caso todas falhem, é importante que o sistema possua capacidade de registrar o passo-a-passo do incidente, de forma que estas informações sirvam para modificar os controles e evitar novos incidentes. Esta é a barreira "**Diagnosticar**".

Slide 29



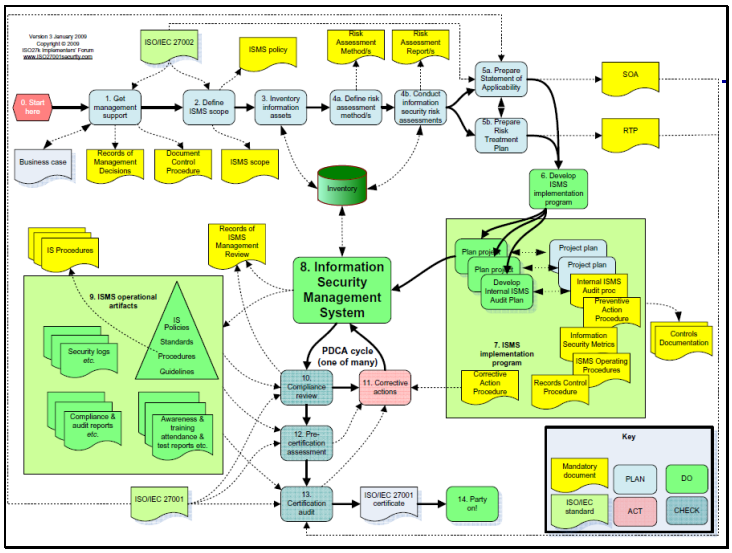
É importante observar que as estratégias de tratamento não são mutuamente excludentes. É possível combinar, por exemplo, controles para modificar o nível do risco, adotando medidas para mitigá-lo e também compartilhar parte do mesmo, como por exemplo fazendo um seguro.

Slide 30



Um SGSI (Sistema de Gestão da Segurança da Informação) é um processo que abrange toda a empresa e seus parceiros, envolvendo: a criação e manutenção de Políticas; atribuição de responsabilidades na Gestão da SegInfo; implantação de programas de educação, treinamento e conscientização; implantação de atividades de Gestão do Risco, envolvendo auditorias periódicas e controle de eventos e incidentes de segurança; monitoramento, medição, análise e avaliação da eficácia do SGSI; e Análise Crítica do SGSI pela Direção da empresa.

Slide 31

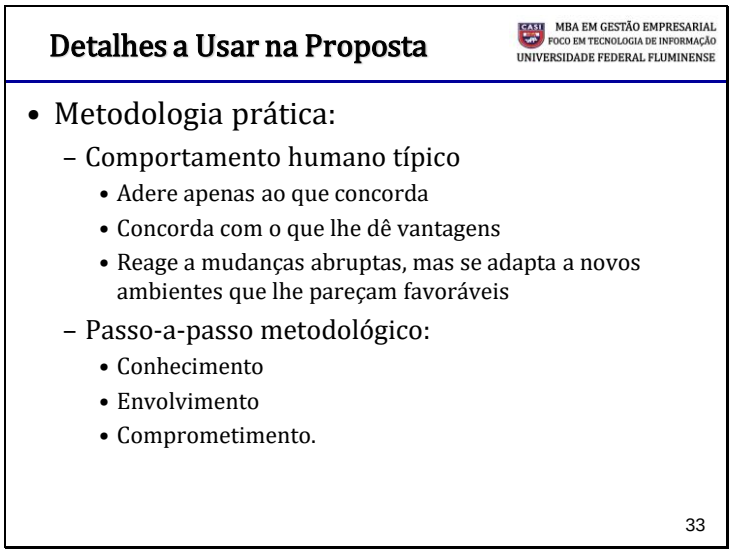


Este é o fluxo da ISO 27001. Esta norma descreve o processo de criação e manutenção de um Sistema de Gestão da Segurança da Informação (SGSI), que se baseia na alteração dos processos da corporação de forma que eles introduzam controles que possibilitem a operação em nível de risco sob controle. Propõe a adoção do ciclo PDCA (PLAN– DO – CHECK – ACT), onde ações de controle do risco seriam propostas com base em requisitos e expectativas em relação ao risco, descritas pelos *stakeholders*. Escopos são definidos, planos são elaborados, garante-se o comprometimento da Direção e alocação de recursos financeiros, pessoais e de material para a criação de uma estrutura para gestão do risco. Elabora-se uma Política de Segurança, que nada mais é do que um conjunto de controles para a Gestão do Risco, e para isso a norma ISO 27002 é a referência, já que descreve as boas práticas para o controle do risco. No final desta fase, descreve-se na Declaração de Aplicabilidade quais controles foram adotados e aqueles que eventualmente deixaram de ser adotados, com as respectivas justificativas, e parte-se para a implementação (DO). A fase CHECK é a responsável pelo monitoramento do nível do risco, através de análises periódicas, e da existência e funcionamento dos controles, através de auditorias. Os resultados desta fase geram propostas de melhorias no sistema (ACT), que provocarão mudanças nos planos e políticas elaborados na fase PLAN.

Slide 32

Existem algumas questões discutíveis no fluxo da ISO 27001. A primeira é que, logo de início, deve-se elaborar a Política de Segurança, em um cenário onde ainda não se sabe onde se quer chegar. Todos estão ainda inseguros quanto ao retorno dos investimentos e a maioria não acredita na eficácia das ações. Na prática, a Política tende a se transformar em "letra morta", ou seja, um manual de regras que ninguém cumpre, iniciando pelos que deveram cobrá-las (os gestores de Processos e a própria direção).
Outra questão é que, já que apenas com o comprometimento da direção da empresa este esforço trará resultados, então convém a adoção de uma fase preliminar de autoconhecimento, onde se busque se dissemine os objetivos do SGSI a implementar, ofereça oportunidades de envolvimento de todos os gestores e se promova a evidenciação de riscos visíveis para todos. Convém que apenas após isso se conduza a discussão de mecanismos de segurança. A implementação do SGSI depende da aprovação CONSCIENTE da direção, e para isso deverão ser estabelecidos objetivos a alcançar, definido o escopo - exigências legais e do negócio, interações com outras áreas de gestão, como a do risco jurídico e o marketing, lista de processos/ativos/sistemas/estrutura organizacional/localização geográfica onde o SGSI será aplicado - e definir papéis e responsabilidades de cada um quanto à SegInfo.
A melhor abordagem é a de fazer um levantamento detalhado e criterioso das ameaças e das vulnerabilidades existentes, com o ENVOLVIMENTO de todos os gestores, elaborar *cases* bem familiares a todos os envolvidos e só então iniciar as mudanças nos processos, o que certamente provocará reações. O processo tende a ser lento e gradual, mas sempre progressivo.

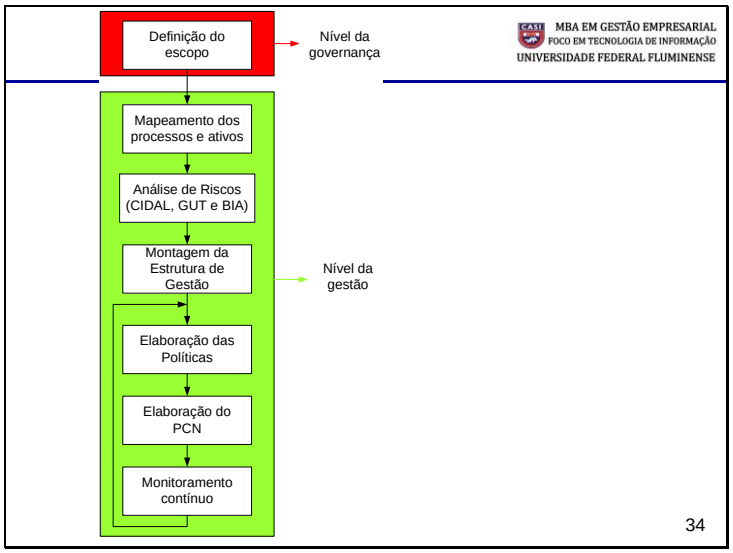
Slide 33



Esta proposta se alinha com a experiência prática do professor nas relações humanas com subordinados por mais de 30 anos. A motivação das pessoas é intrinsecamente relacionada com punições e recompensas. É essencial que seja deixado claro para todos o que ELES (e não a empresa) GANHAM com esta mudança, e o que eles PERDEM em caso de descumprimento de regras. Grandes empresas, como a IBM, por exemplo, premiam colaboradores que se destacam nas aferições de *compliance* com viagens curtas para locais aprazíveis com a família, motivando os colaboradores a não se envergonharem por terem um comportamento ético, que não é comum na cultura latina.

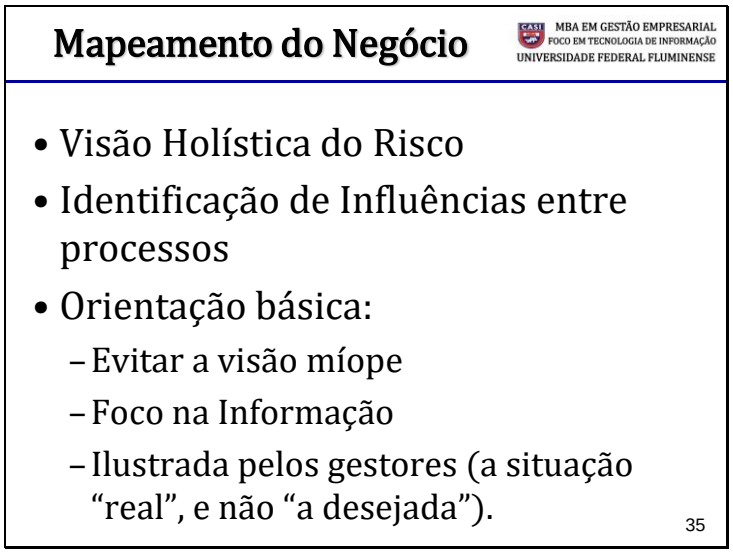
Para o ser humano REALMENTE mudar o seu comportamento quanto à qualquer aspecto, é essencial que ele inicialmente COMPREENDA o que isso significa, saiba como fazer do jeito certo e identifique (concordando, naturalmente) o que é errado. Chamamos isso de fase de **CONHECIMENTO**, feita objetivamente através de educação, treinamento e conscientização. É importante aferir se este nível foi alcançado, antes de partir para a próxima etapa, que é a do **ENVOLVIMENTO**. Nela, busca-se familiarizar o colaborador com nossos objetivos, oferecendo oportunidades para a sua participação no processo. Pede-se a sua opinião, e premia-se de alguma forma quem vem contribuindo na elaboração dos planos. É importante tentar usar as ideias dos colaboradores o máximo possível da forma que eles idealizaram, para que eles se tornem "donos" da ideia. A última e mais importante fase é a do **COMPROMETIMENTO**, onde TODOS, gestores e colaboradores, cumprem e cobram o cumprimento das políticas, não apenas porque são regras, mas porque ACREDITAM nas regras.

Slide 34



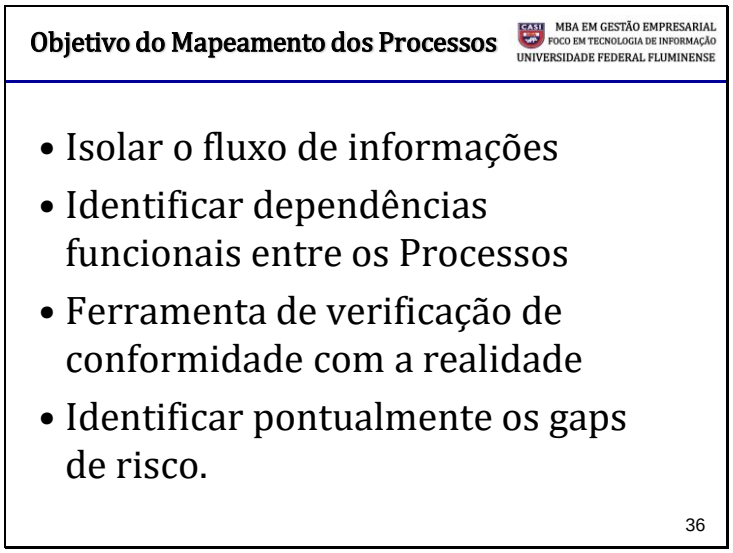
Este fluxo sintetiza as ações a empreender. Importante ressaltar que tudo se inicia pela definição do escopo, onde o negócio define os critérios de aceitação de risco, e tudo será desenhado em função destes limites. A partir daí as fases são complementares, sempre usando os resultados da fase anterior na próxima. No monitoramento contínuo, novos riscos evidenciados demandam novas análises de risco e até mesmo o redimensionamento da estrutura de gestão, porém este ciclo é o mais genérico e aplicável no trabalho inicial.

Slide 35



Mapear o negócio significa evidenciar o fluxo da informação. Não adianta proteger a informação em um momento do seu ciclo de vida e deixá-la exposta nos demais.
Durante a fase de coleta das informações para o mapeamento, é fundamental evitar a visão míope típica dos gestores muito atarefados. Eles vão evidenciar apenas aquilo que é mais visível e cotidiano, e normalmente as vulnerabilidades existem também em outros momentos menos visíveis. Observe o caso da quebra de sigilo na prova do ENEM de 2009, que ocorreu dentro da gráfica que imprimiu as provas (serviço terceirizado pela CESPE, elaboradora da prova). É vital que TODO o ciclo da informação seja mapeado.
O foco desta fase não é na produtividade, lucro, redundâncias operacionais, e sim na Segurança da Informação, então a informação deve ser o foco da proteção. Os aspectos do negócio são levados em consideração apenas na hora de evidenciar os requisitos e os impactos.
Outra questão comum é a descrição pelos gestores de um cenário fantasioso, baseado no que eles gostariam que seus processos fossem, e não o que eles realmente são. É importante não criticar, não demonstrar reprovação ou espanto com a descrição feita pelos gestores, de forma que possamos mapear a situação REAL, e não uma situação desejada.

Slide 36

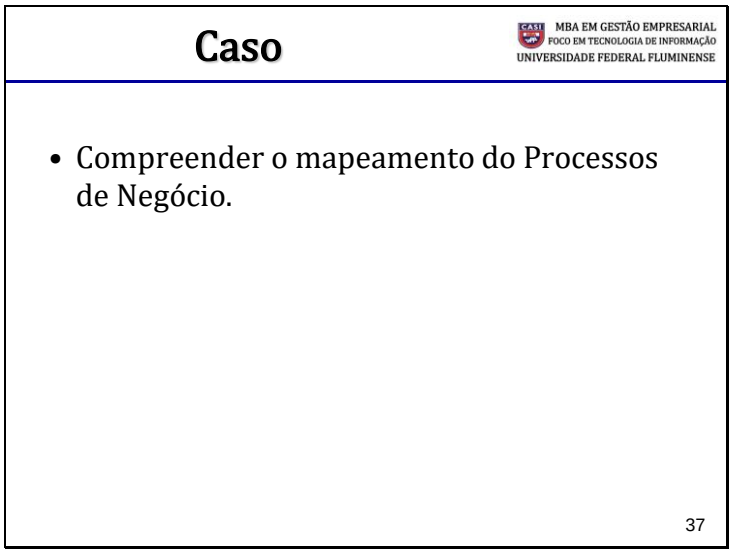


Outro aspecto relevante aqui são as interações entre os processos. Mais adiante, vamos ver que precisaremos identificar tolerâncias temporais de processos, e não costuma ocorrer uma definição adequada destas tolerâncias pelas empresas. Observe o seguinte: normalmente, quem define a autonomia de um sistema de nobreak é o gestor de TI, mas ele é o menos indicado para fazer isso. Como TI APOIA processos, ele deve identificar junto aos processos apoiados qual é a necessidade da manutenção de operacionalidade dos recursos de TI de cada um deles em situação de crise, com o objetivo de minimizar os impactos de acordo com os critérios de aceitação de risco, para então decidir. Esta pergunta feita aos gestores sem uma predefinição do que significa "quanto tempo os serviços de TI devem permanecer disponíveis em uma situação de crise" sempre redundará na resposta "SEMPRE", se não houver uma compreensão adequada que há um custo bastante importante para alta disponibilidade.

Como o mapeamento gera um modelo físico, um mapa fácil de compreender, é bastante produtivo apresentar o resultado de cada processo para seus componentes. É bastante comum a intervenção de colaboradores indicando que aquela não é a realidade. Com isso vamos depurando o modelo até convergir para o que é efetivamente praticado.

Atualmente, técnicas disponíveis como o BPMN e UML são bastante adequadas para este trabalho.

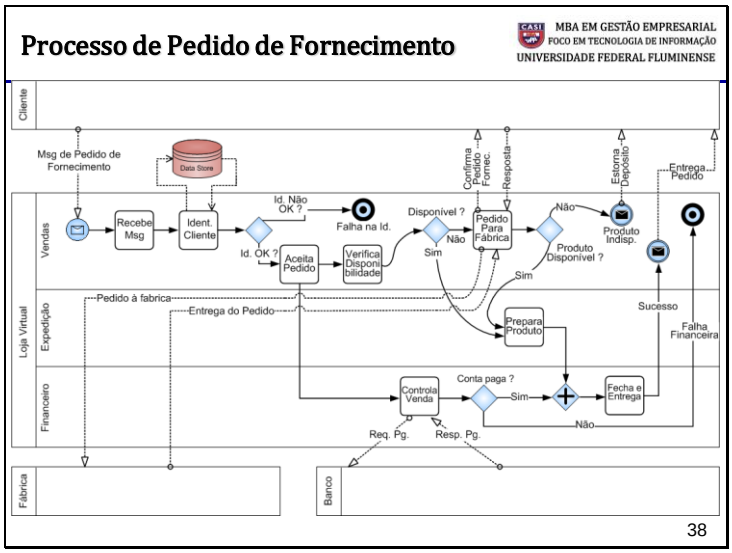
Slide 37



Como foge ao escopo do curso as técnicas de mapeamento de processos, vamos apenas compreender o mapeamento fornecido no case, acompanhando o fluxo de informações entre os processos, identificando dependências funcionais e evidenciando situações de risco. Observe as interações entre os atores CLIENTE, VENDAS, EXPEDIÇÃO, FINANCEIRO, FÁBRICA e BANCO, bem como os seus respectivos processos internos. No case, podemos perceber, que há várias vulnerabilidades. Por exemplo, se uma ameaça forjar **Resp. Pg.** do banco, pode provocar a entrega de produtos sem que o pagamento tenha sido realizado.

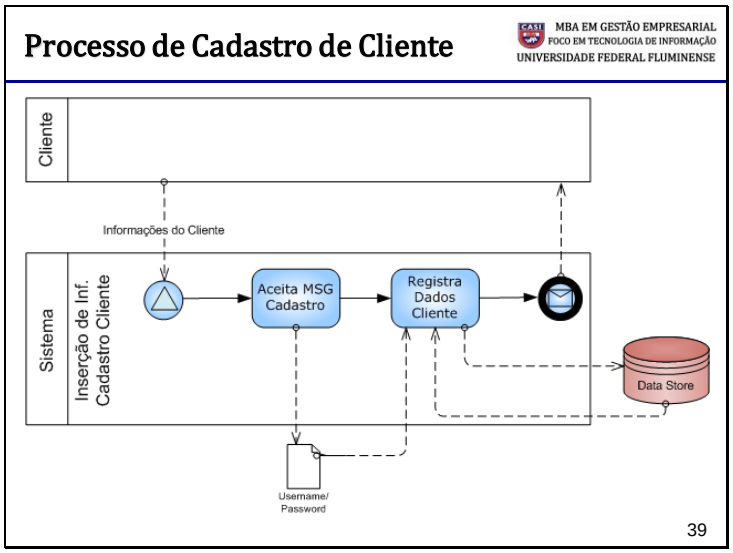
Para possibilitar a Gestão da Segurança da Informação, é vital que os processos estejam documentados. Para a maioria das empresas, este será o primeiro passo a empreender. Outra demanda que facilita o desenvolvimento deste trabalho é a existência de um Planejamento Estratégico para a empresa. A Governança e a Gestão precisam andar juntas.

Slide 38



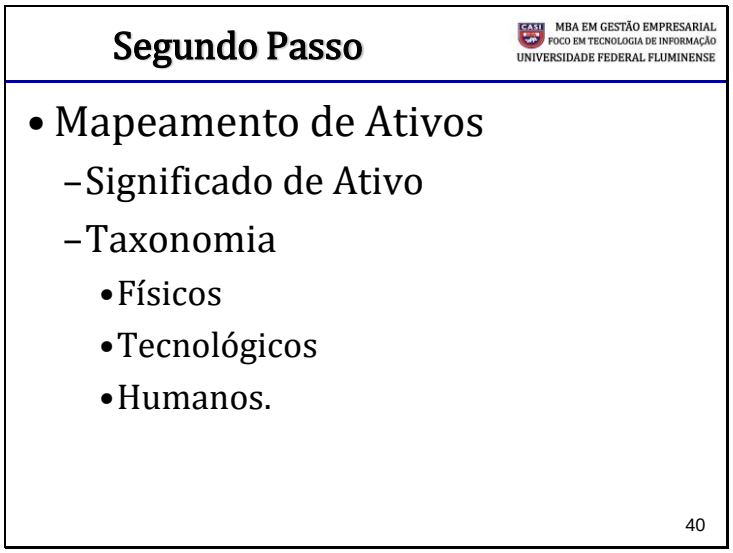
Este modelo, feito em BPMN, permite a evidenciação do fluxo da informação dentro do processo. Com isso, é mais visível a existência de gaps e vulnerabilidades. Outra vantagem deste modelo é a visualização das interfaces entre os atores do processo em análise.

Slide 39



Este é o processo de cadastramento do cliente, que evidencia o armazenamento de um login/senha local. Esta é uma vulnerabilidade frequente, como disseminado em http://www.baguete.com.br/noticias/06/05/2014/ingresso-com-falhas-graves-de-seguranca , onde o famoso ingresso.com criptografaria apenas algumas informações dos clientes, deixando, no entanto, as senhas armazenadas em *plain-text*.

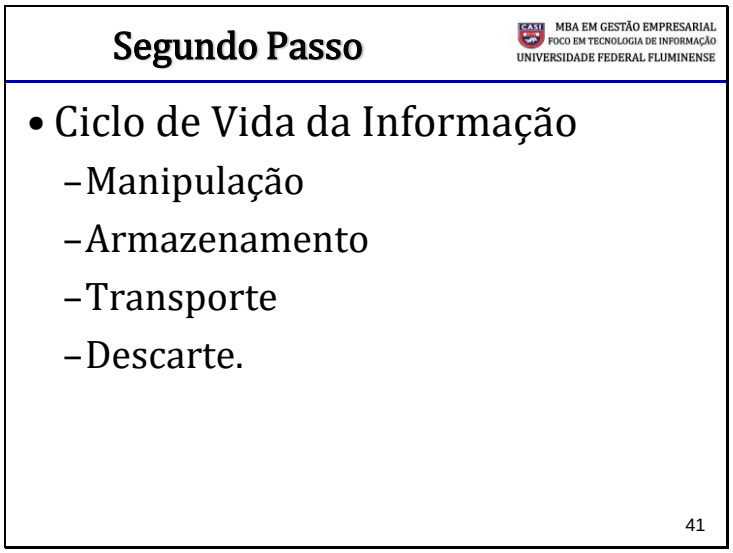
Slide 40



Após descrever o fluxo das informações, passamos para a fase do mapeamento dos ativos. Apesar do foco deste trabalho ser a informação, ela é manipulada, armazenada, transportada e descartada por ativos, então eles devem ser identificados para que possam ser usados no desenvolvimento dos nossos controles. Os ativos da empresa também devem estar disponíveis e com competência adequada para garantir a produtividade esperada.

Da mesma forma que as ameaças, os ativos também são classificados de acordo com suas respectivas naturezas, já que as soluções são tipicamente do mesmo tipo, mas nada impede que usemos soluções tecnológicas para controle de ativos humanos, por exemplo.

Slide 41



A **Manipulação** é a fase onde as informações são CRIADAS ou ALTERADAS. Não se separa estas operações em fases diferentes no ciclo de vida porque os controles são idênticos, como por exemplo através de ferramentas de controles de direitos de acesso à informação.

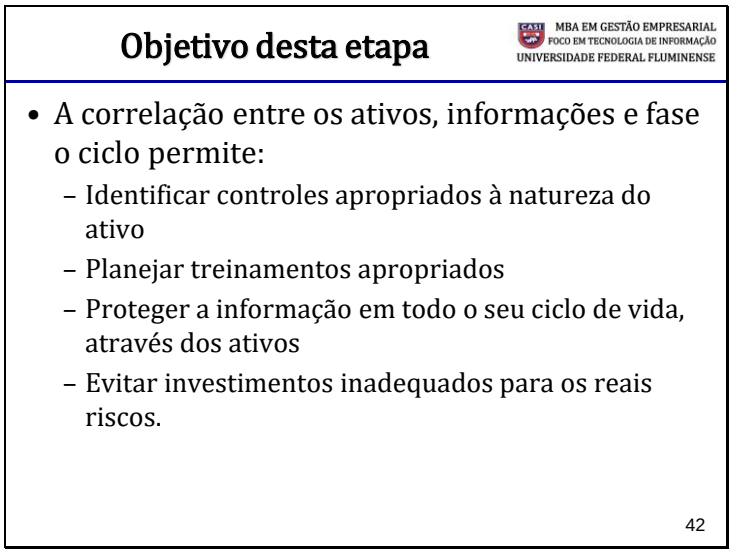
O **Armazenamento** é a fase onde as informações estão depositadas em repositórios permanentes ou voláteis, acessíveis para o acesso. Quando uma pessoa assimila informações estratégicas em sua memória e depois de transfere para outra empresa, a fase sob risco é o armazenamento, e não o transporte. Por isso, se há conhecimento estratégico para a empresa o mesmo deve ser segmentado, para evitar que uma única pessoa possa reproduzi-lo em outra empresa. Contratos e "quarentenas" não tem funcionado na maioria dos casos.

O **Transporte** é a fase onde a informação está sendo transportada através de um meio físico entre dois pontos, e pode ser acessada por terceiros. Equipamentos de conectividade e a rede transportam informação.

O **Descarte** é a fase onde as informações são eliminadas do sistema processual. É talvez a mais negligenciada de todas nas empresas.

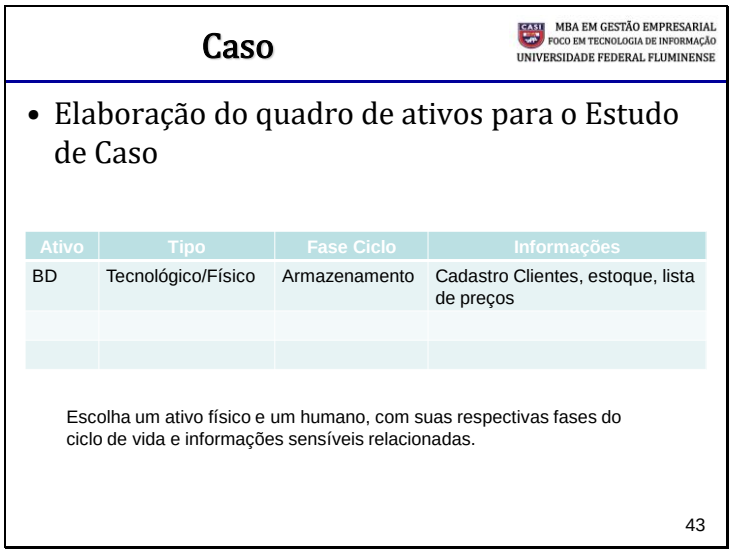
Um exemplo: um computador não manipula informações, ele apenas armazena. Quem manipula são as pessoas, através do desenvolvimento de sistemas, ou de operadores, realizando transações.

Slide 42



Visando minimizar os custos com os controles, possibilitar que eles sejam eficientes e eficazes, além de oferecer uma nítida percepção de utilidade para todos é vital que façam sentido e tenham utilidade imediata. Treinamentos, por exemplo, são feitos nas empresas sem planejamento, capacidade de aferição de resultados e, principalmente, motivação adequada. É preciso evitar este efeito.

Slide 43



Caso

MBA EM GESTÃO EMPRESARIAL
FOCO EM TECNOLOGIA DE INFORMAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

- Elaboração do quadro de ativos para o Estudo de Caso

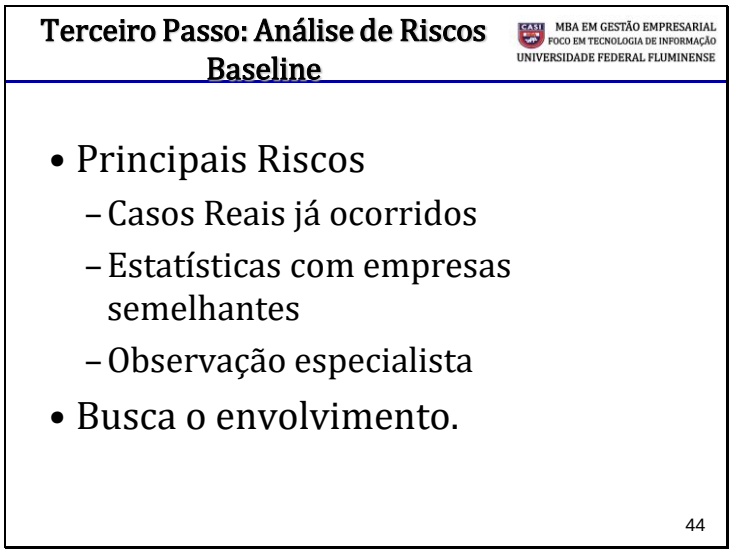
Ativo	Tipo	Fase Ciclo	Informações
BD	Tecnológico/Físico	Armazenamento	Cadastro Clientes, estoque, lista de preços

Escolha um ativo físico e um humano, com suas respectivas fases do ciclo de vida e informações sensíveis relacionadas.

43

Convém que os ativos pertencentes às atividades processuais sejam identificados e classificados de acordo com a taxonomia proposta. Eles serão o foco das ações de controle e de contingenciamento. Vamos preencher no *template* no fim da apostila a tabela reproduzida acima, com base nos ativos essenciais para a operação de uma Loja Virtual. Estes ativos podem ser físicos, tecnológicos ou humanos.

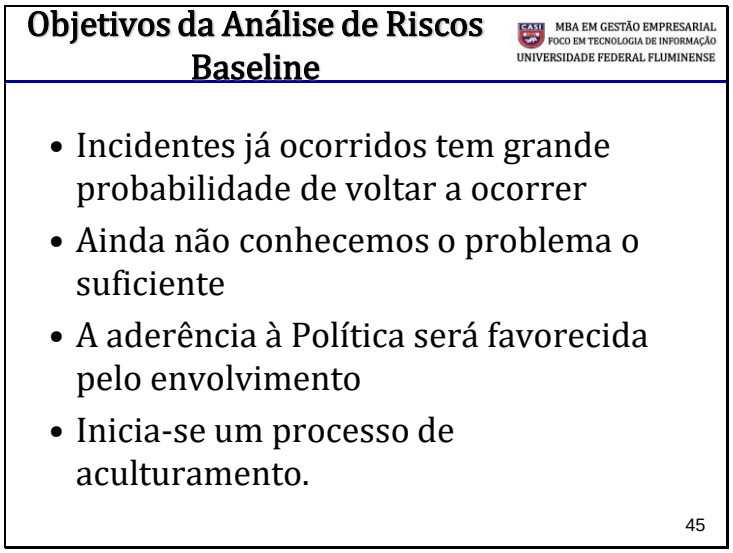
Slide 44



Neste passo, vamos nos focar nas situações mais visíveis para qualquer colaborador da empresa, sempre na busca do envolvimento do mesmo. Situações que ele já vivenciou são perfeitas. Ele tem condições de emitir opiniões, porque tem em sua memória detalhes familiares importantes para evitar que os incidentes voltem a ocorrer. Com isso ele se torna coautor das propostas e facilitamos a obtenção do seu interesse na formação de cultura de segurança. Incidentes já ocorridos com outras empresas também costumam ser bem aceitos por todos.

A palavra do gestor do processo (observação especialista) é também buscada e valorizada, uma vez que seu comprometimento futuro é essencial para o sucesso do trabalho de formação de cultura de segurança, e ao priorizarmos as suas opiniões, facilitamos o seu envolvimento.

Slide 45



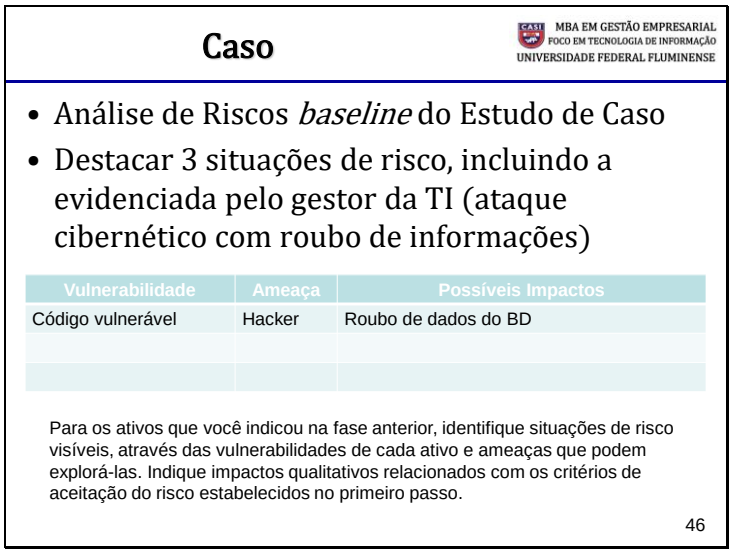
É fato que, na cultura latina, não há tipicamente um retorno das "lições aprendidas" para o ambiente de produção. As pessoas são, em geral, supersticiosas e atribuem os incidentes a fatores subjetivos, como o "azar", "inveja" e outros. Acreditam também que "um raio não cai duas vezes no mesmo lugar", e que já aprenderam com o incidente e por isso ele não voltará a ocorrer. Na prática, não há um esforço de análise das razões do incidente nem a proposição de mudanças que proporcionem um ambiente mais seguro.

Visando mudar esta cultura, os incidentes já ocorridos são inicialmente priorizados, já que as condições ambientais (ameaças e vulnerabilidades) estiveram presentes e o seu encontro culminou em um incidente, sendo então bastante razoável acreditar que ele voltará a ocorrer, caso não haja mudança de cultura e a adoção de controles específicos para este caso.

Outra questão relevante é que a gestão do risco em Segurança da Informação é disciplina nova para a maioria dos gestores, e é essencial para que eles mudem de comportamento que estejam motivados. Um dos fatores da motivação é a nítida compreensão do problema. Situações indiscutíveis de risco facilitam este entendimento.

Outro aspecto é que nesta fase do trabalho ainda não há maturidade suficiente para se eleger incidentes prováveis. Isto apenas terá bons resultados mais adiante, após a obtenção do envolvimento de todos e do comprometimento ao menos de todos os gerentes.

Slide 46



Caso

MBA EM GESTÃO EMPRESARIAL
FOCO EM TECNOLOGIA DE INFORMAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

- Análise de Riscos *baseline* do Estudo de Caso
- Destacar 3 situações de risco, incluindo a evidenciada pelo gestor da TI (ataque cibernético com roubo de informações)

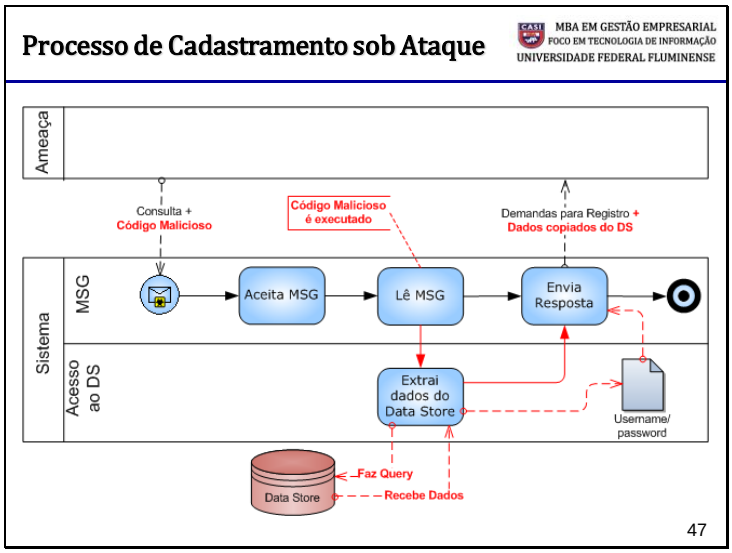
Vulnerabilidade	Ameaça	Possíveis Impactos
Código vulnerável	Hacker	Roubo de dados do BD

Para os ativos que você indicou na fase anterior, identifique situações de risco visíveis, através das vulnerabilidades de cada ativo e ameaças que podem explorá-las. Indique impactos qualitativos relacionados com os critérios de aceitação do risco estabelecidos no primeiro passo.

46

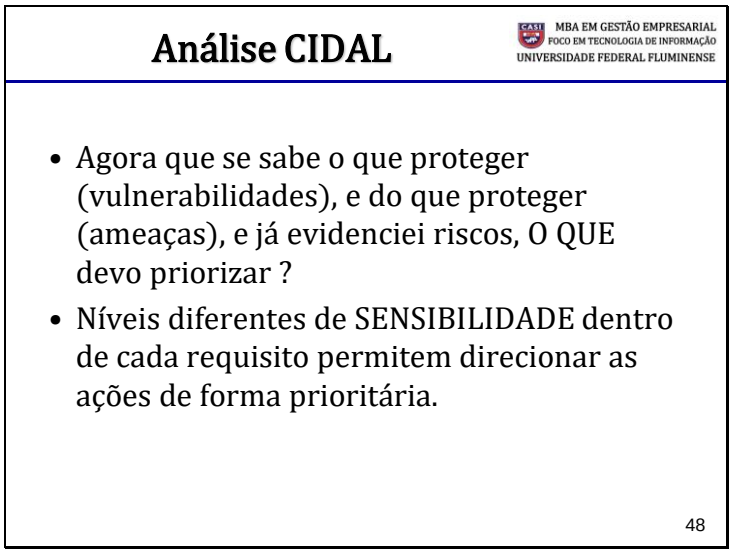
Com base no texto apresentado, destaque situações de risco. Acrescente à tabela do *template* mais dois tipos de risco evidenciados, preferencialmente um com vulnerabilidade humana e outro de natureza física. Para cada um deles identifique os impactos decorrentes, ainda de forma qualitativa.

Slide 47



Este slide ilustra a situação evidenciada pelo gestor de TI. Ao testar a interface de cadastramento de cliente, verificou-se que o código é sujeito ao *SQL Injection*, que é uma vulnerabilidade através da qual podem ser inseridos comandos em linguagem SQL para evidenciar senhas, nomes de usuários e até mesmo fazer login no sistema como administrador sem a necessidade de conhecer a senha. Há vários tutoriais disponíveis através da internet para que até mesmo leigos possam realizar este tipo de ataque.

Slide 48



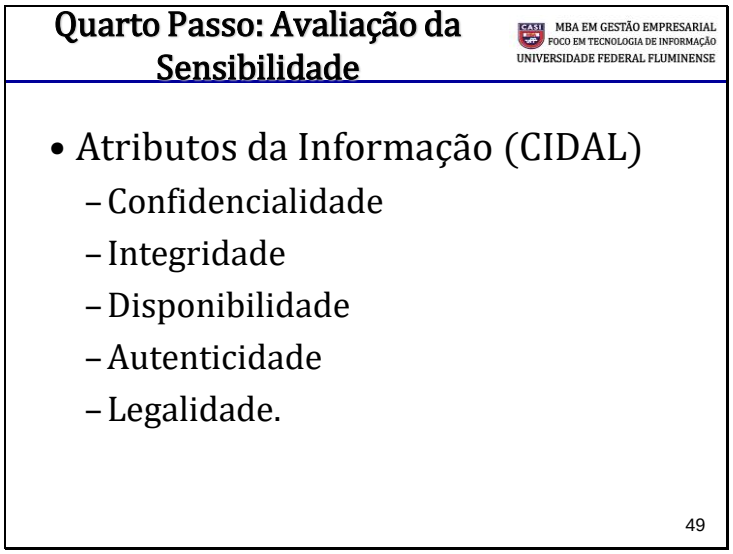
Análise CIDAL, acrônimo para os principais atributos da informação, **Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade**, é a próxima etapa deste trabalho de criação de cultura de segurança e a busca do envolvimento/comprometimento do pessoal. Toda informação tem sensibilidade aos atributos, mas a criticidade dos mesmos é variável. No primeiro passo identificamos a sensibilidade que implica em risco, para em seguida avaliar o nível de criticidade.

Confidencialidade é a materialização do princípio "necessidade de conhecer". Em estrito interesse no negócio, apenas os colaboradores que PRECISEM de acesso às informações para executar suas atividades processuais devem tê-lo. Além disso, as informações devem ser classificadas de acordo com o seu valor estratégico para a corporação, e quanto mais estratégicas e valiosas, mais protegidas elas devem ser. Para isso, devem ser definidos níveis de confidencialidade diferentes para informações de valores diferentes, para que possamos protegê-las de forma proporcional ao seu valor. A ISO 27002:2013 recomenda que a informação seja classificada de acordo com o seu "valor, requisitos legais, sensibilidade e criticidade para a organização, para evitar modificação ou divulgação não-autorizada". Esta classificação também deve abranger os atributos Integridade e Disponibilidade.

Integridade é um atributo que visa garantir que uma informação não possa ser alterada ou corrompida em trânsito entre uma origem e um destino, ou seja, por alguém não autorizado.

A **Disponibilidade** é, segundo a ISO 27001:2013, é a propriedade de uma informação "estar acessível e utilizável sob demanda por uma entidade autorizada". Para estar disponível, os atributos Confidencialidade e Integridade devem estar previamente garantidos. Continua →

Slide 49



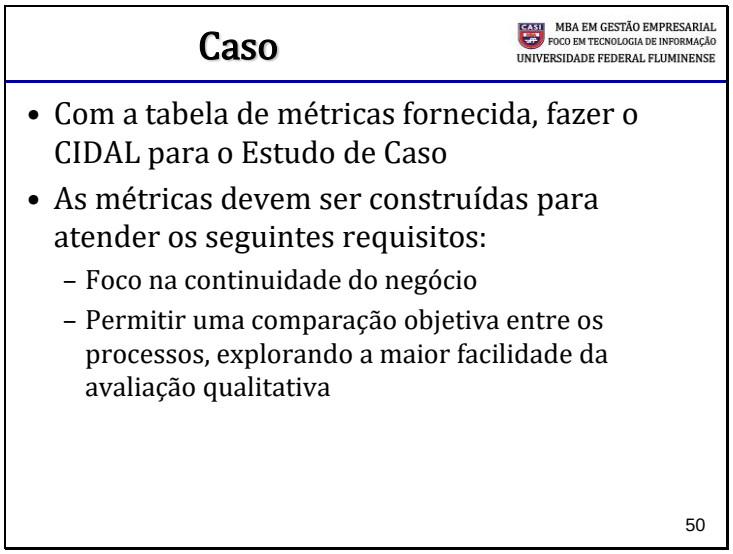
A definição destes três atributos (CID) apresenta uma lacuna: nos três, é necessário que se esteja devidamente IDENTIFICADO e AUTORIZADO para usufruir do direito ao acesso à informação. Por conta disso, usamos também na Análise de Sensibilidade e Criticidade os atributos:

Autenticidade – É a garantia de que uma informação é proveniente da fonte que se declara ter sido responsável pela sua geração ou alteração. Observe que um "login" é uma informação, cuja confirmação de identidade é feita através de uma senha pessoal privada, logo, é um mecanismo de autenticidade. Mas também podemos garantir a autenticidade de documentos e arquivos, com o uso de mecanismos criptológicos.

A **Legalidade** é outro aspecto importante, porque muitas vezes as fraudes são cometidas por pessoas que efetivamente tinham direitos de realizar transações, mas não possuíam os diplomas legais para fazê-las. Imagine um gestor financeiro de uma empresa, responsável pelo pagamento de contas. É trivial para ele realizar transações fraudulentas, transferindo recursos da empresa para sua conta pessoal ou de terceiros. Isso não configura incidente de autenticidade, porque ele possui credenciais para realizar transferências de recursos, nem de integridade, porque não foram feitas alterações em trânsito, e sim na sua própria origem. O incidente é de LEGALIDADE, porque o que ele fez fere os princípios éticos e de fidelidade do colaborador para com a empresa.

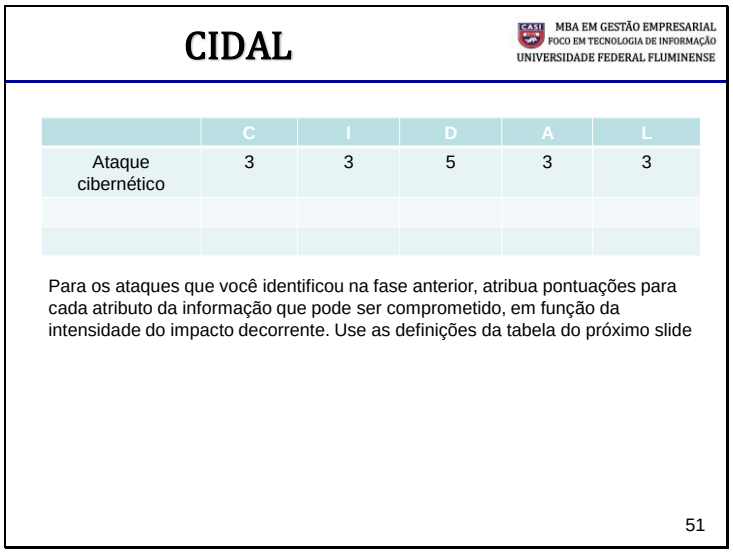
O incidente do pagamento de um prêmio de 73 milhões da mega-sena pela CEF de Tocantinópolis (http://glo.bo/1hBXTtG) é um exemplo. Não havia mecanismo algum que impedisse que um gerente desonesto cometesse a fraude. Como isso nunca havia acontecido, o processo era simples e direto. Em nossa abordagem, possuía vulnerabilidades processuais, e pela dimensão dos impactos, o processo deveria ter sido remodelado para EVITAR/ELIMINAR o risco. Hoje a CEF exige que os prêmios sejam validados pela direção de jogos antes de ser pago.

Slide 50



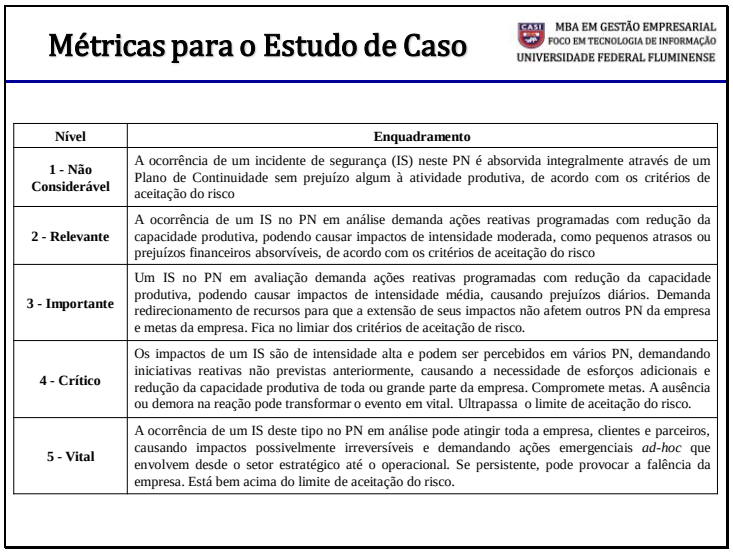
É muito mais fácil identificar isoladamente a sensibilidade de cada processo com base em parâmetros e depois compará-los do que tentar identificar qual processo é mais sensível em um grupo de processos. Torna o trabalho mais técnico e isento de vieses causados por percepções equivocadas. Outra questão é a necessidade do uso de uma métrica para esta avaliação. Conforme dito anteriormente, será adotada a métrica qualitativa, mais simples de usar e mais alinhada com o pensamento humano. Após a maturidade deste processo, a migração para a quantitativa se tornará possível pela inserção nos processos do hábito de se registrar eventos e incidentes de segurança.
A discussão em torno da aferição da sensibilidade também é muito agregadora por estimular uma discussão que aumenta o nível de maturidade dos envolvidos e contribui para a formação da cultura de segurança. A orientação é sempre buscar a aferição em relação aos requisitos e expectativas do negócio, estabelecidas no início do trabalho.

Slide 51



Vamos agora preencher a tabela CIDAL no template. A orientação é sempre buscar a aferição em relação aos requisitos e expectativas do negócio, estabelecidas no início do trabalho, e a tabela de correspondência entre efeitos impactantes com um número entre 1 a 5. Esta tabela está disponível no próximo slide.
Justificativas para o exemplo:
Um ataque cibernético pode ser feito de várias formas. Pode, por exemplo, consistir em uma invasão para cópia dos cadastros (ataque à confidencialidade). Pode também ser efetuado para alteração de dados do banco, fraudando boletos, transferências financeiras e afins (ataque à integridade) ou até mesmo a destruição de dados (ataque à integridade). Uma forma mais simples e comum seria a sobrecarga do sistema através de milhares de solicitações forjadas, inundando o sistema e incapacitando-o a atender às solicitações legítimas (ataque à disponibilidade). No exemplo acima a avaliação subjetiva é baseada em situações já ocorridas e de domínio público, como a da Sony, referenciada no Estudo de Caso. Um incidente de disponibilidade afeta TODOS os usuários e possui ampla visibilidade. Os outros tipos de incidentes são tipicamente tratados através da troca de senhas e procedimentos adicionais aos processos de compra, como por exemplo a confirmação telefônica de uma compra, já feita normalmente por várias empresas (exemplo: Grupo C&C). Por conta disso, e da indicação pela direção da empresa da inadmissibilidade de interrupção da Loja Virtual, a DISPONIBILIDADE foi considerada VITAL e para os demais atributos IMPORTANTE, de acordo com as definições da tabela do próximo slide.

Slide 52



Métricas para o Estudo de Caso

MBA EM GESTÃO EMPRESARIAL
FOCO EM TECNOLOGIA DE INFORMAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

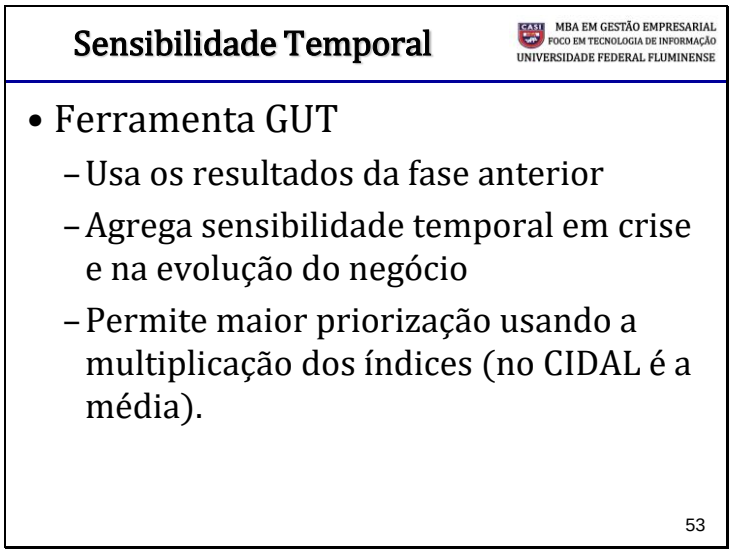
Nível	Enquadramento
1 - Não Considerável	A ocorrência de um incidente de segurança (IS) neste PN é absorvida integralmente através de um Plano de Continuidade sem prejuízo algum à atividade produtiva, de acordo com os critérios de aceitação do risco
2 - Relevante	A ocorrência de um IS no PN em análise demanda ações reativas programadas com redução da capacidade produtiva, podendo causar impactos de intensidade moderada, como pequenos atrasos ou prejuízos financeiros absorvíveis, de acordo com os critérios de aceitação do risco
3 - Importante	Um IS no PN em avaliação demanda ações reativas programadas com redução da capacidade produtiva, podendo causar impactos de intensidade média, causando prejuízos diários. Demanda redirecionamento de recursos para que a extensão de seus impactos não afetem outros PN da empresa e metas da empresa. Fica no limiar dos critérios de aceitação de risco.
4 - Crítico	Os impactos de um IS são de intensidade alta e podem ser percebidos em vários PN, demandando iniciativas reativas não previstas anteriormente, causando a necessidade de esforços adicionais e redução da capacidade produtiva de toda ou grande parte da empresa. Compromete metas. A ausência ou demora na reação pode transformar o evento em vital. Ultrapassa o limite de aceitação do risco.
5 - Vital	A ocorrência de um IS deste tipo no PN em análise pode atingir toda a empresa, clientes e parceiros, causando impactos possivelmente irreversíveis e demandando ações emergenciais *ad-hoc* que envolvem desde o setor estratégico até o operacional. Se persistente, pode provocar a falência da empresa. Está bem acima do limite de aceitação do risco.

Esta tabela de métricas vem sendo usada como ponto de partida para criação de tabelas personalizadas pelo professor em trabalhos de consultoria, na fase preliminar. Naturalmente deve ser adaptada em função das peculiaridades do negócio, mas é um bom começo. Observe que a avaliação é absolutamente qualitativa, e há diferenciais fundamentais entre os diferentes níveis de sensibilidade. A sugestão, via de regra, é de que processos que sejam, ao final da análise, classificados como VITAIS ou CRÍTICOS sejam contingenciados, além da adoção de controles. Isto os tornaria IMPORTANTES, RELEVANTES ou NÃO CONSIDERÁVEIS, em função do volume de recursos investidos no tratamento do risco. Já os processos classificados como NÃO CONSIDERÁVEL a IMPORTANTE demandariam apenas ações de controle, por estarem dentro do limite aceitável de risco.

Como para priorizar são necessários diferentes índices de sensibilidade, são atribuídos os valores de 1 a 5 nesta fase, de acordo com o constatado.

Observe a diferença, ainda que sutil, entre os níveis IMPORTANTE e CRÍTICO. No IMPORTANTE, há ações planejadas para o incidente, mas pela sua criticidade são necessários esforços adicionais em relação aos níveis anteriores, paralisando as atividades cotidianas normais e passando para uma operação em crise. No entanto, estes esforços são suficientes para evitar que a extensão de seus impactos não afete outros Processos de Negócio. Já o CRÍTICO é um processo não contingenciado, com inter-relações de dependência com outros processos, de forma que sua deficiência operativa afeta outros processos. Reduz a capacidade de produção e compromete metas. Um Plano de contingência deve ser elaborado para que, no mínimo, este processo deixe de ser crítico e passe a ser importante.

Slide 53

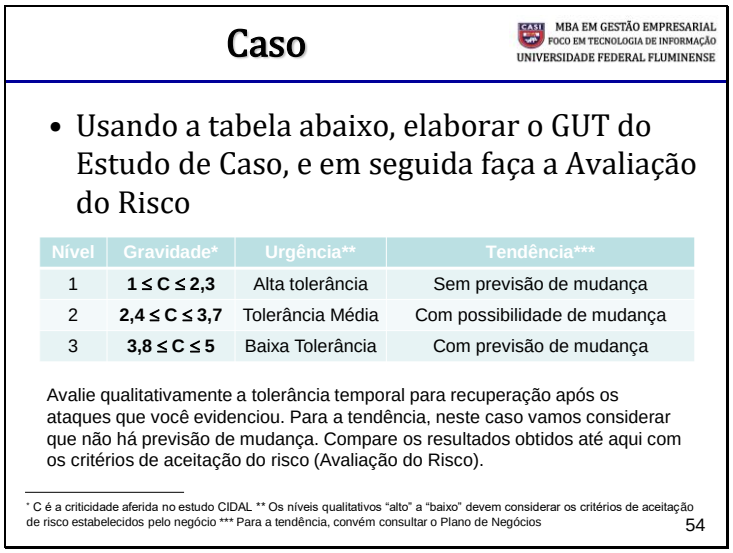


Nesta fase, os resultados da fase anterior, aonde vamos ter muitos resultados próximos com a tabela CIDAL, vão ser complementados com uma análise temporal do processo. São basicamente duas análises:

- **URGÊNCIA** – Durante a crise, como o incidente agrava a capacidade de manutenção operacional do negócio ao longo do tempo? Qual é o limite temporal ideal para que o processo seja contingenciado, de forma a minimizar os efeitos do incidente? Sabemos que hoje, com as redes sociais, as notícias se propagam muito rapidamente, e dependendo do incidente a empresa precisa ter respostas rápidas para evitar efeitos irreversíveis. No campo operacional, é fácil obter esta resposta através dos SLA firmados com os clientes.
- **TENDÊNCIA** – Muitas vezes quando fazemos uma análise, o processo é pouco crítico, mas há conhecimento de mudanças que vão torná-lo mais crítico ao longo do tempo. Fusões, aquisições e investimentos normalmente provocam mudança no nível de criticidade de alguns processos, e isso tem que ser identificado com antecedência, priorizando o processo e o preparando com antecedência para esta nova realidade. Esta variável permite isso.

O GUT então é a multiplicação dos resultados de CRITICIDADE, que aqui, por mera intenção de não reinventar a roda, já que o GUT é conhecido e utilizado em outras áreas, vamos usar os resultados como a variável G (de GRAVIDADE), com os de urgência e de tendência. Obviamente precisaremos de métricas para a avaliação da Urgência e da Tendência, obtidas dentro do próprio ambiente operacional de cada empresa.

Slide 54



Caso

MBA EM GESTÃO EMPRESARIAL
FOCO EM TECNOLOGIA DE INFORMAÇÃO
UNIVERSIDADE FEDERAL FLUMINENSE

- Usando a tabela abaixo, elaborar o GUT do Estudo de Caso, e em seguida faça a Avaliação do Risco

Nível	Gravidade*	Urgência**	Tendência***
1	**1 ≤ C ≤ 2,3**	Alta tolerância	Sem previsão de mudança
2	**2,4 ≤ C ≤ 3,7**	Tolerância Média	Com possibilidade de mudança
3	**3,8 ≤ C ≤ 5**	Baixa Tolerância	Com previsão de mudança

Avalie qualitativamente a tolerância temporal para recuperação após os ataques que você evidenciou. Para a tendência, neste caso vamos considerar que não há previsão de mudança. Compare os resultados obtidos até aqui com os critérios de aceitação do risco (Avaliação do Risco).

* C é a criticidade aferida no estudo CIDAL ** Os níveis qualitativos "alto" a "baixo" devem considerar os critérios de aceitação de risco estabelecidos pelo negócio *** Para a tendência, convém consultar o Plano de Negócios

54

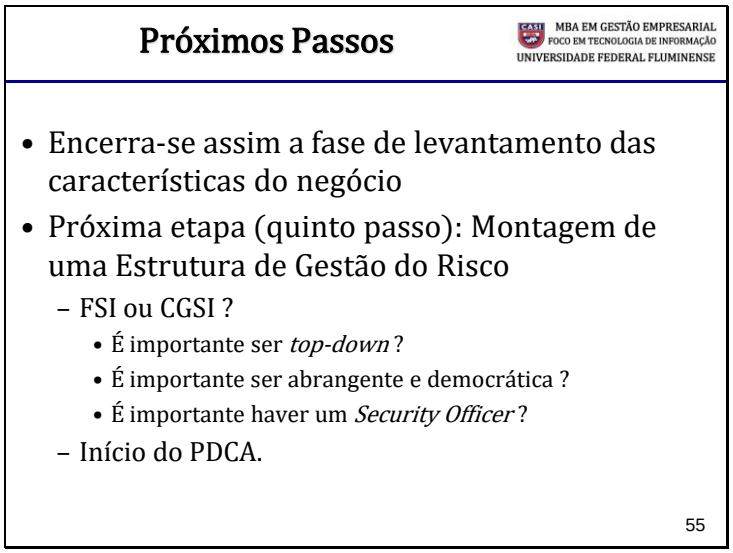
Vamos agora para a tabela GUT no template. Para este exercício, adotou-se apenas 3 níveis. Naturalmente, com a criação de cultura e o hábito de registrar eventos e incidentes de segurança, estas tabelas de métricas (CIDAL e GUT) poderão evoluir para um modelo quantitativo com maior granularidade, que é o ideal.

Como a Criticidade no CIDAL tinha sido avaliada em 5 níveis, foi necessária uma conversão de 1 a 5 para 1 a 3, conforme a primeira coluna da tabela. Na segunda coluna, **a urgência** pode ser aferida qualitativamente, de acordo com comparações objetivas entre as situações de risco, usando a relação entre o tempo decorrido em situação de crise e o efeito impactante. **A tendência** é a análise da iminência de mudança do nível de risco do processo em avaliação ao longo do tempo, de forma que ele possa estar preparado quando sua criticidade se agravar. Uma boa fonte de informações sobre esta situação é o Plano de Negócios da empresa, onde a existência de ações que POSSIBILITEM o agravamento do risco no processo multiplicaria a criticidade do mesmo por dois (duplicaria), e a PREVISÃO de agravamento triplicaria o índice de criticidade.

Após isso, ainda na mesma página do template, faça a Avaliação do Risco e decida a forma de tratamento.

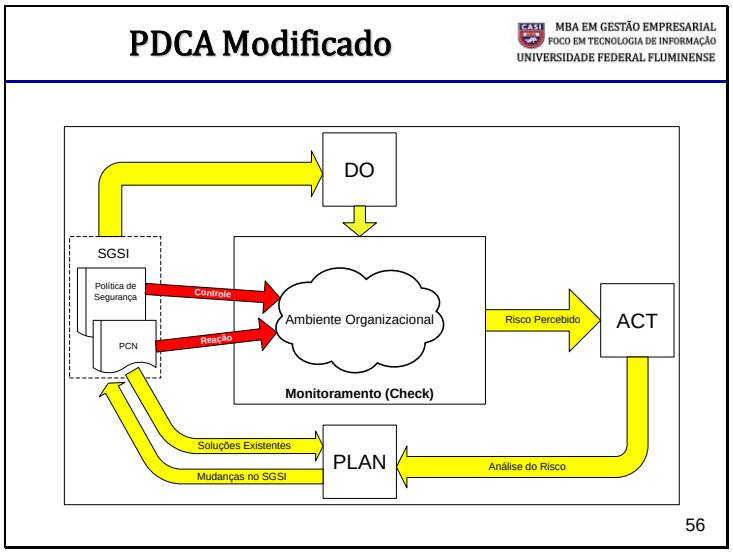
A Avaliação do Risco é a comparação dos Riscos evidenciados e os resultados de sua análise com os CRITÉRIOS de aceitação do risco estabelecidos pelo negócio. Com base nisso, uma proposta de tratamento deve ser feita (Ações de Modificação, Retenção, Eliminação ou Compartilhamento – que podem ser combinadas). Além disso, se o risco estiver acima do nível aceitável, o processo deverá ser contingenciado. Esta proposta se materializará na Política de Segurança e/ou no Plano de Continuidade dos Negócios (PCN).

Slide 55



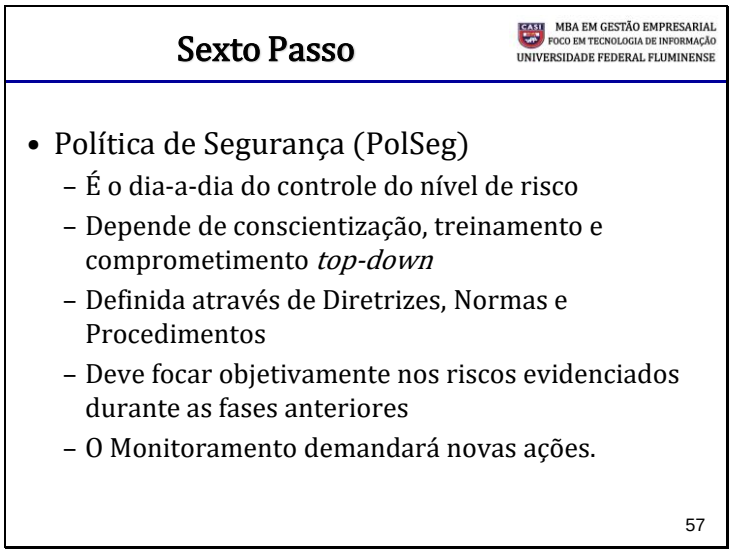
Após este levantamento preliminar, passamos a uma fase onde algumas ações deverão ser materializadas. A primeira delas é a criação de uma estrutura para a Gestão de Segurança da Informação, composta, minimamente, de um *Security Office* – setor especificamente criado para monitorar o ambiente e garantir a existência e a operação dos controles. É responsável também pela manutenção da rotina de treinamento e capacitação. Deve ter perfil executivo e sua célula funcional deve ser independente de qualquer setor operacional da empresa. Deve estar ligado diretamente ao Conselho Executivo. Muitas empresas implementam este setor juntamente com Auditoria e *Compliance*. Apesar da criação desta célula de negócio, a responsabilidade pela existência e a evolução (com melhorias) da Gestão da Segurança é da direção da empresa e não pode ser repassada para setor algum. Da mesma forma, as atividades de segurança devem ser coordenadas por representantes dos diferentes setores da organização, que devem assumir papéis e funções relevantes. As normas sugerem que isso seja atingido através do CGSI (Comitê Gestor da Segurança da Informação). Minha sugestão é que este comitê se amplie para um Fórum de Segurança da Informação (FSI). A diferença é que um comitê, por definição, é composto por um número finito e com membros fixos, o que dificulta a participação, envolvimento e por fim o comprometimento de todos. O fórum é mais democrático, abre a possibilidade da participação de todos os interessados, facilitando a criação da cultura de segurança.

Slide 56



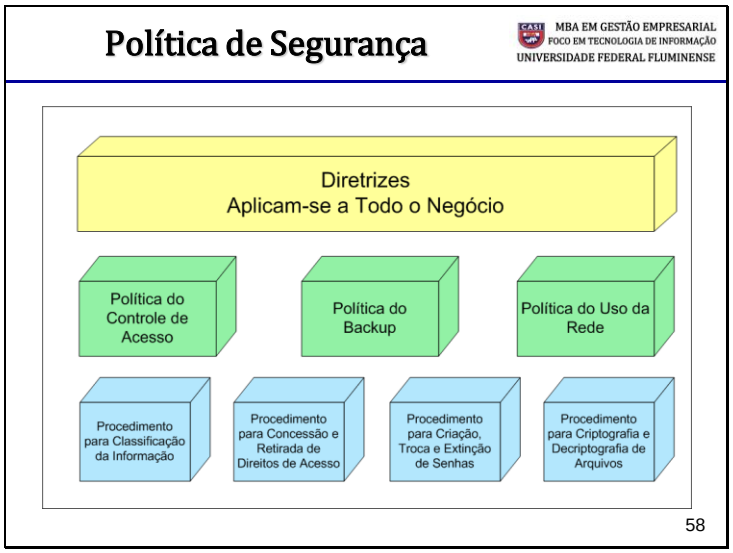
O ciclo de Deming tradicional, adotado na ISO 27001, sugere uma ação cíclica, onde no início deve-se planejar soluções (fase PLAN). Mas planejar soluções para que? Claro que temos expectativas e requisitos que devem ser alcançados, mas os controles são aplicados em função da existência ou não de riscos nos processos de negócio. Minha sugestão é a da adoção de um PDCA modificado, onde o centro de tudo é o ambiente, onde os riscos são identificados através de um contínuo monitoramento. Estes riscos são analisados e avaliados, à luz dos critérios de aceitação de riscos (que devem ser definidos pela direção), aí sim demandando ações de planejamento. Estas ações são definidas em função do que já existe na empresa (no SGSI), e eventuais alterações necessárias devem ser imediatamente documentadas no mesmo, após aprovadas pela direção. As ações aprovadas e documentadas são então implementadas no ambiente, gerando imediatos efeitos de monitoramento, que já se atualizou junto ao SGSI.
O ciclo tradicional de Deming é perfeito para a gestão da qualidade, onde produtos são idealizados, fabricados e vendidos, e a aceitação ou rejeição pelo consumidor deve rapidamente ser monitorada e o produto melhorado para buscar a satisfação do consumidor. Em segurança a coisa é bem diferente.

Slide 57



Após identificar a demanda de contingenciamento dos processos críticos e vitais, a definição dos controles da Política de Segurança é o próximo desafio. Relembrando o que já foi dito anteriormente, alguns cuidados são necessários para evitar que a Política se torne "letra morta". O primeiro deles é que os controles devem ser justificados, então devem ser direcionados para riscos reais existentes e visíveis. O segundo é que a Política deve ser cumprida por todos na empresa, do diretor ao colaborador mais subalterno. O terceiro é que a política deve ser modularizada, para que os colaboradores possam conhecer as regras e serem treinados apenas no que é pertinente às suas funções e o seu nível de acesso. O quarto e último cuidado básico é que não se deve ter a obsessão de definir toda a Política em um único esforço. Costumo dizer que o ótimo é inimigo do bom, então é mais interessante iniciar com uma política simples e objetiva, com poucas regras que sejam compreendidas e praticadas por todos do que uma política grande e complexa que ninguém segue.
Uma Política é composta de DIRETRIZES, NORMAS e PROCEDIMENTOS.

Slide 58



A Política de Segurança da empresa torna clara e documentada a posição estratégica dos objetivos de segurança da Informação da Direção, com respeito à operação de um SGSI. Além disso, é importante que se deixe claro o que acontece quando a Política não é seguida. A ISO 27003:2011 dá instruções detalhadas sobre o processo de criação dos documentos da Política.

Uma forma atual de desenvolver as **Diretrizes** é estruturar a Política de acordo com o seguinte exemplo:

1 – Resumo da Política. Ex.: A Informação deve ser protegida por todos da empresa durante todo o seu ciclo de vida, independentemente de sua forma;

2 – Introdução. Ex.: A Informação pode estar em forma digital, impressa ou falada. A SegInfo é a proteção contra ameaças que podem afetar o negócio;

3 – Escopo. Ex.: Esta Política se destina a proteger a informação de acordo com os requisitos de seus atributos;

4 – Objetivos. Ex.: Os Riscos de SegInfo devem ser identificados, compreendidos e tratados para se tornarem aceitáveis, segundo os critérios do negócio;

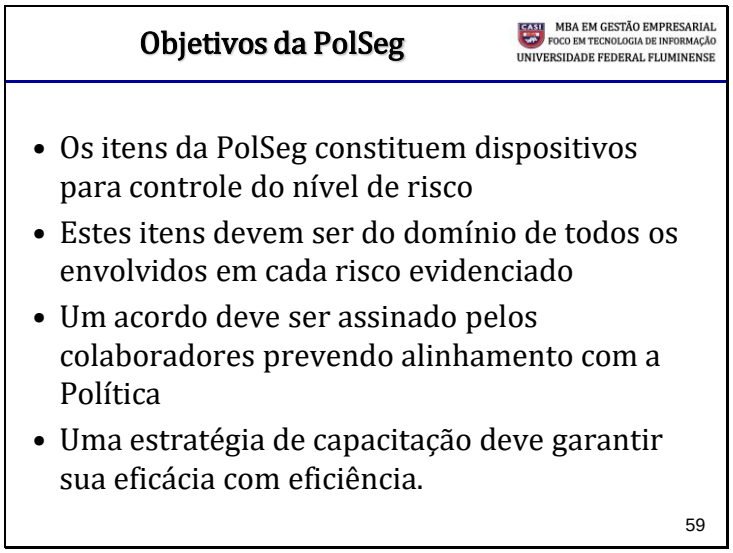
5 – Princípios (Critérios para atingir os Objetivos). Ex.: Todos os riscos devem ser objeto de Análise e Avaliação de Risco pelos Gestores de Processos. As métricas para a Avaliação do Risco estão declaradas na Política dos Critérios de Aceitação de Risco;

6 – Responsabilidades. Ex.: Cada funcionário, terceiro ou parceiro tem responsabilidades de SegInfo como parte da execução de seus trabalhos;

7 – Resultados. Ex.: Incidentes de Segurança não afetarão a saúde financeira nem a imagem da empresa de forma relevante; e

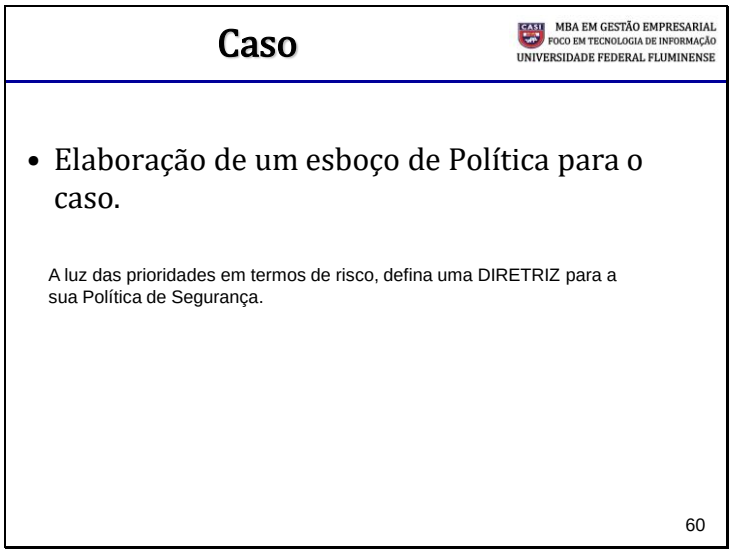
8 – Políticas Relacionadas. Ex.: Política dos Critérios de Aceitação do Risco.

Slide 59



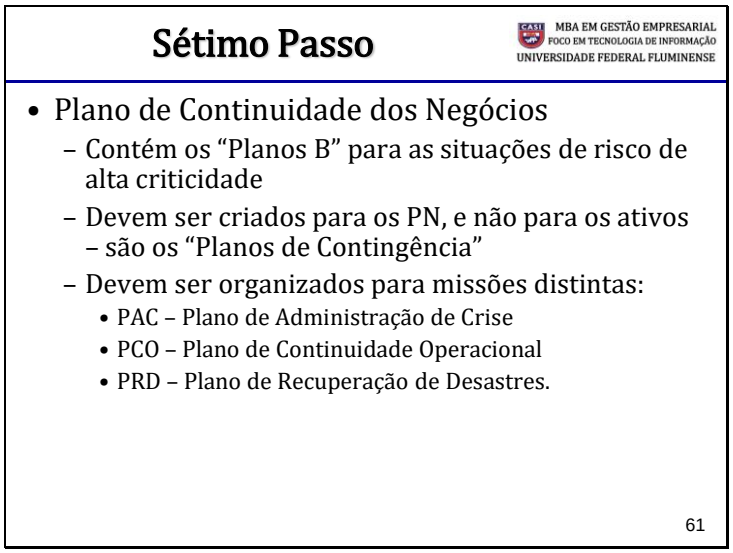
As entradas na Política devem ser elaboradas com a finalidade de controlar o risco, então devem ser construídas com base nos registros disponíveis no Plano Diretor de Segurança elaborado até então. A estratégia de capacitação deve ser planejada e executada de forma que todos conheçam suas responsabilidades e estejam comprometidos com o seu cumprimento. É também importante que a Política tenha registros acerca de um processo de punição para quem descumpre a Política.
Em resumo, pode-se dizer que:
DIRETRIZES – São aplicáveis a todos os setores da corporação. Por isso, são genéricas e descrevem apenas o que fazer, sem detalhar como fazer;
NORMAS – São políticas setoriais, ou seja, detalham como cada diretriz deve ser alcançada em cada processo. Também podem ser construídas como Políticas de um processo de SegInfo específico, como ilustrado no slide 58 para a TI; e
PROCEDIMENTOS – Detalham o passo-a-passo de como atingir os objetivos de cada política.
Exemplo: Uma DIRETRIZ diz que a proteção de informações sensíveis deve ser praticada por todos na empresa; uma NORMA sobre o controle do acesso à informação, na parte referente à salvaguarda de informações sigilosas, define que informações classificadas como confidenciais devem ser criptografadas; e um PROCEDIMENTO descreve a metodologia adotada pela empresa para avaliar a sensibilidade e rotular a informação, para que cada proprietário da informação possa praticá-lo.

Slide 60



Vamos agora para o template definir um dos componentes da Política de Segurança decorrente do trabalho que foi feito até agora. A sugestão é que se foque no risco e se defina uma DIRETRIZ, que é parte da Política.

Slide 61



O Plano de Continuidade dos Negócios é prioritário neste momento, uma vez que existem processos críticos e vitais que não possuem contingências. Este plano pertence à empresa, então ele não deve ser relacionado a um Centro de Custo específico, e sim ao Centro de Custo do PCN empresarial.

Visando atingir eficácia com eficiência, sugerimos modularizar o PCN por Planos de Contingência, focados em atividades específicas do negócio que devem ser mantidas minimamente operacionais para preservar os interesses do negócio. Deve possibilitar treinamentos curtos e monitoráveis, com atores e objetivos muito bem definidos.

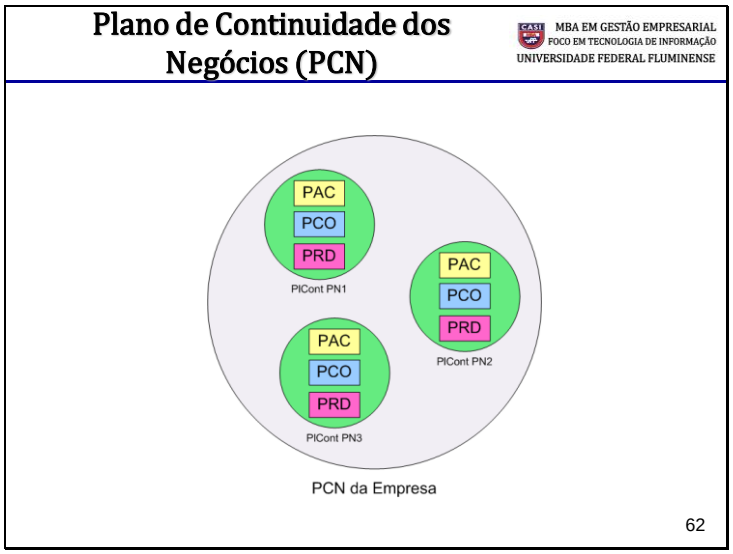
Para isso, adotamos a seguinte divisão dos Planos de Contingência:

PAC – Plano de Administração de Crise – Parte responsável pela definição dos atores e se seus eventuais substitutos; identificação dos recursos necessários para a solução contingencial e a localização dos mesmos; e identificação das ações de comunicação com as partes interessadas;

PCO – Plano de Continuidade Operacional – Deve ser focado no processo, e não nos ativos. Núcleo do plano, define minuciosamente as ações que visam a garantia da operação da atividade de negócio, independente da perda de ativos por conta de incidentes, ou seja, define uma alternativa de funcionamento. É importante observar que, quanto menos tolerante à redução de operacionalidade, mais caro será o contingenciamento, então é mister a identificação adequada dos níveis mínimos e ideais de operacionalidade, para racionalizar os investimentos em contingenciamento.

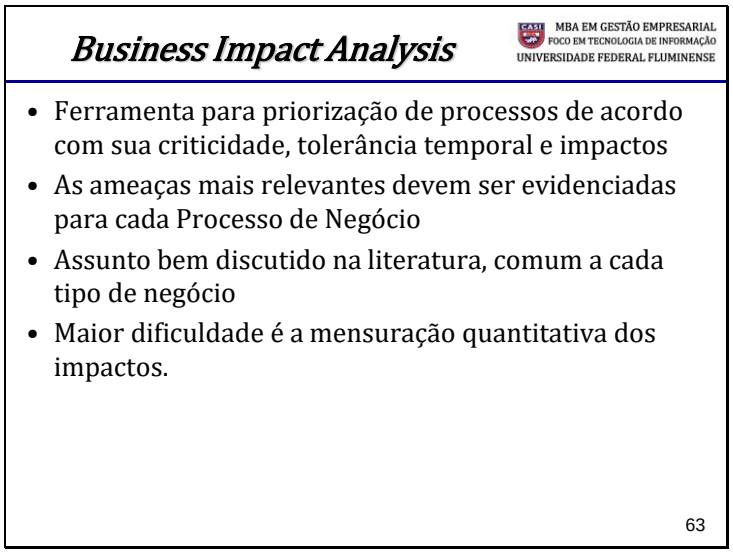
PRD – Plano de Recuperação de Desastres – É a parte do Plano que se preocupa com a recuperação dos ativos comprometidos, mas também tem suma importância pela responsabilidade pela identificação das razões que culminaram com a ocorrência do incidente e a proposição de mudanças nos controles que evitem que ele volte a ocorrer.

Slide 62



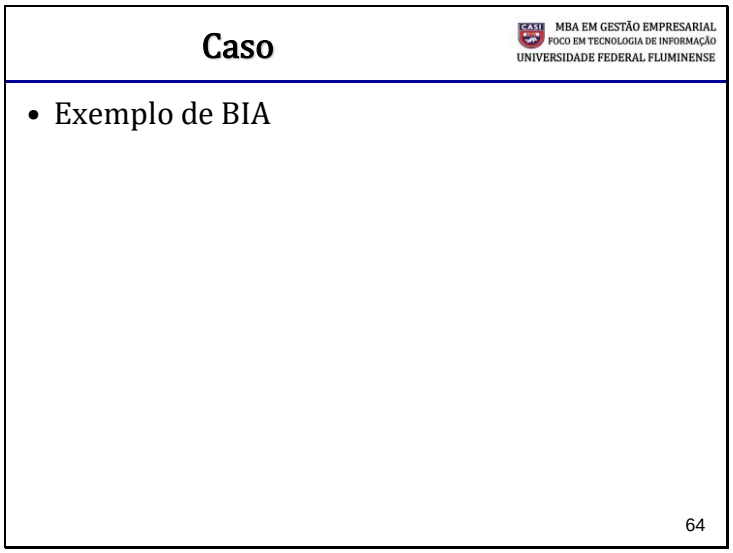
Esta figura ilustra o discurso anterior, onde a modularização é feita em busca da racionalização dos esforços e investimentos em ações de contingenciamento. É importante que a empresa possa ter um único *Budget* para Continuidade dos Negócios.

Slide 63



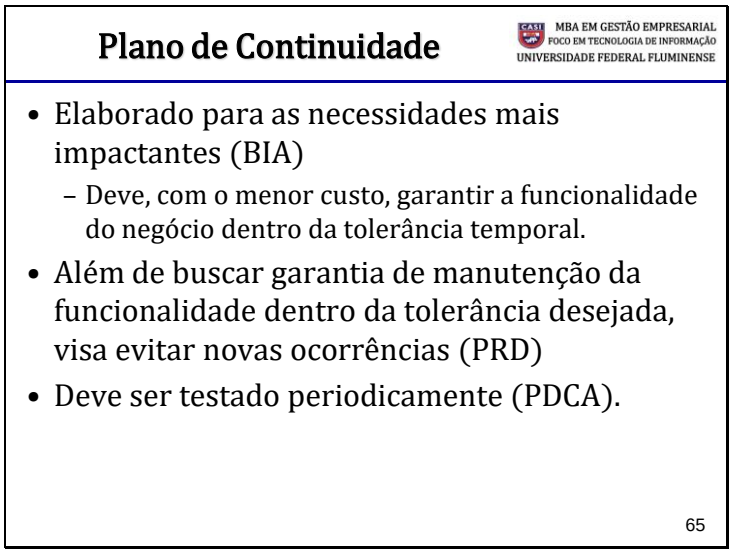
O BIA é mais uma ferramenta conhecida que pode ser usada neste ponto da análise para possibilitar o aumento da precisão da priorização já realizada, mas para isso depende de uma mensuração quantitativa dos impactos, o que nem sempre é trivial por conta da parcela intangível do mesmo. Não vamos usá-la neste curso, exatamente por termos adotado a abordagem qualitativa.
Outra utilidade é a identificação pontual de ameaças que devem ser usadas como ponto de partida para a definição das ações de contingenciamento, apesar disso nem sempre ser necessário, já que o foco é a manutenção de operacionalidade da atividade do negócio, independentemente da razão que o tornou indisponível.

Slide 64



Ao migrar para a análise de risco quantitativa, que é dependente de números precisos para a Probabilidade de Ocorrência e o valor impactante, este instrumento se torna mais útil para a tomada de decisão, mas isso depende substancialmente da criação da cultura de segurança, que proporcionará o hábito do registro de eventos e incidentes de segurança, além da contabilização de impactos financeiros em exercício de "lições aprendidas", bem como o desenvolvimento de uma sensibilidade para a tolerância temporal.

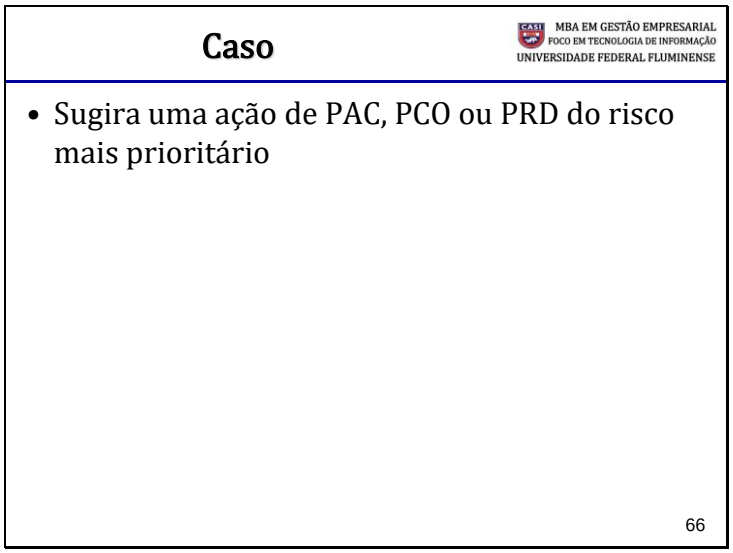
Slide 65



Para o direcionamento de recursos para o desenvolvimento de uma solução de contingenciamento, convém comparar estes custos com o potencial prejuízo que a empresa pode vir a ter com um incidente, naturalmente considerada a sua probabilidade de ocorrência. Obviamente, todo investimento em tratamento de riscos deve ser compatível com o impacto estimado. Muitas empresas não tratam riscos ambientais no Brasil porque as multas são baixas e a consciência do povo nesta área ainda é pequena.

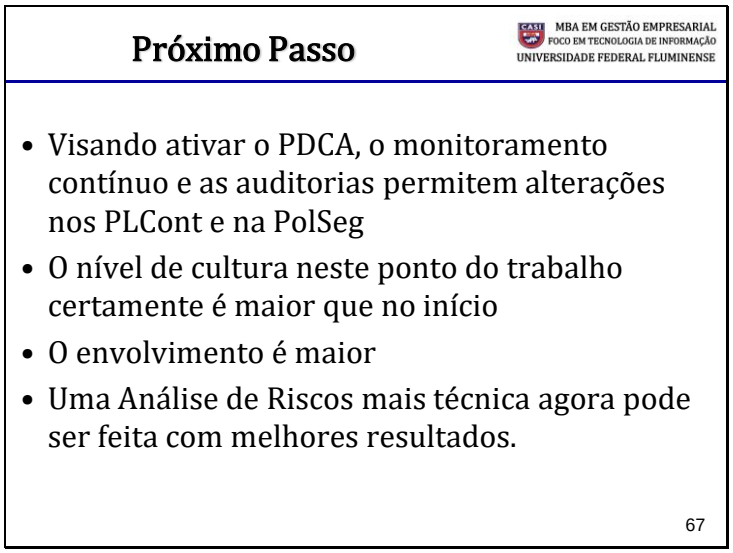
Uma questão-chave nos Planos de Contingência é o treinamento. É fundamental que todos os envolvidos estejam CAPACITADOS para executarem suas respectivas funções na solução de contingência. Observa-se, até em grandes empresas, que os planos até existem, mas não há treinamento, porque ele é previsto no próprio Plano de Contingência. Treinamento é ação de MODIFICAÇÃO (MITIGAÇÃO) de risco, então os treinamentos devem ser obrigatórios, periódicos e previstos na POLÍTICA DE SEGURANÇA. Seus resultados devem ser documentados e avaliados, para que os próximos treinamentos sejam focados no aprimoramento dos resultados. Com isso, os resultados dos treinamentos passarão a ser verificados nas auditorias e a eficácia dos planos passará a ser possível.

Slide 66



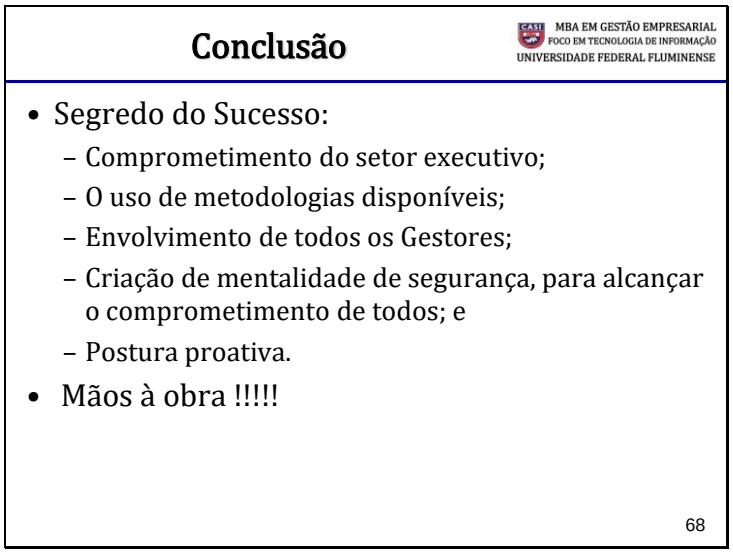
Para encerrar o trabalho, preencha no *template* uma ação de PAC, PCO ou PRD que faria parte do Plano de Contingências para o risco mais prioritário que você evidenciou.

Slide 67



Inevitavelmente, após esse ciclo da maturidade, todos estarão mais conscientes da importância da gestão do risco e com maior capacidade para interpretar os resultados de riscos identificados através de seus componentes. Deixa de ser algo arbitrário que é lembrado esporadicamente por alguém, para ser um processo técnico, com a evidenciação objetiva de vulnerabilidades existentes e ameaças possíveis, com uma mensuração menos incerta dos impactos. Mensurar significa “reduzir incerteza”, e para isso é necessário coletar informações do ambiente. O monitoramento contínuo é fundamental, para que se possa evidenciar mudanças ambientais, com a consequente mudança no nível de risco. Estas mudanças devem ser analisadas e as possíveis implicações nas soluções de contingenciamento de processos críticos e os controles devem ser reavaliados.

Slide 68



Para complemento da nota, siga minhas instruções em sala de sala. Você deverá acrescentar mais um modelo analítico ao case realizado em sala.

Em caso de dúvidas, não hesite em me procurar através do email fred@sauersecurity.com.br

3. 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 no template do final da apostila são:

1. **Definição de um Critério de Aceitação do Risco**, com base na documentação do anexo deste estudo de caso e as orientações disponíveis no slide 18 do material teórico;
2. **Mapeamento dos Ativos** no Processo ilustrado no Caso. Com base na figura 1, identificar ativos que podem ser comprometidos causando impactos;
3. **Mapeamento dos Riscos** – Partindo da identificação das Vulnerabilidades;
4. **Fazer a Análise CIDAL** do processo, com base nos riscos evidenciados na fase anterior;
5. **Fazer a Análise GUT** – Inserir aspectos temporais nas demandas para recuperação do processo e na evolução da criticidade do processo no Plano de Negócios da empresa;
6. **Fazer a Análise do Risco** – Comparar os riscos evidenciados com os critérios de aceitação de risco e decidir qual caminho tomar.
7. **Definir uma DIRETRIZ da Política de Segurança** desta empresa, à luz dos riscos evidenciados; e
8. **Propor uma ação de Continuidade dos Negócios**, enquadrando-a adequadamente (PAC, PCO ou PRD).

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 Gestão da 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 B2C[1]. 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

[1] B2C – Business to Consumer

ser um excelente mercado para empresas exclusivamente virtuais, como a AliBaba e o Mercado Livre.

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

No caso da Loja Virtual deste Estudo de Caso, a falta de planejamento, bem como de envolvimento de todos os setores e principalmente do comprometimento dos especialistas em TI com a Segurança da Informação provocou o lançamento de uma plataforma problemática, sujeita a ataques. A plataforma de compras online usa códigos antigos já prontos e não 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 que sempre falo em sala...).

Ocorre que, em virtude de incidentes de segurança da informação graves, como os do Ingresso.com, LinkedIn, Sony e vários outros, surgiu uma nova demanda de negócio pela certificação ISO 27001, bem como o interesse pela adoção de *frameworks* como o PCI, CoBIT e ITIL, e 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 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.

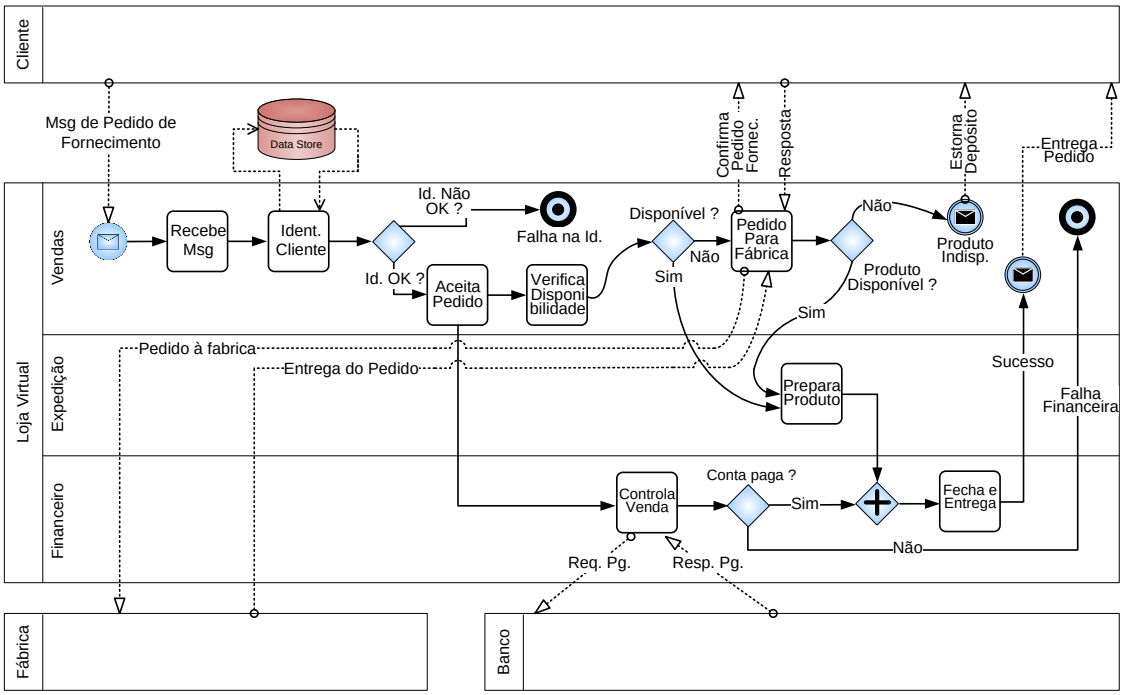


Figura 1 - Modelo em BPMN da Loja Virtual

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.

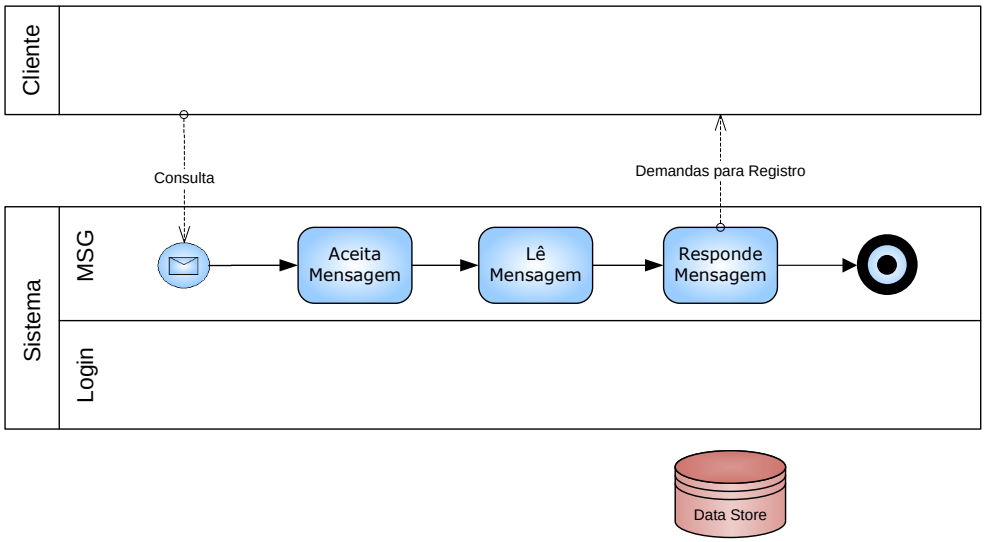


Figura 2 - Consulta para Pedido de Cadastro

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.

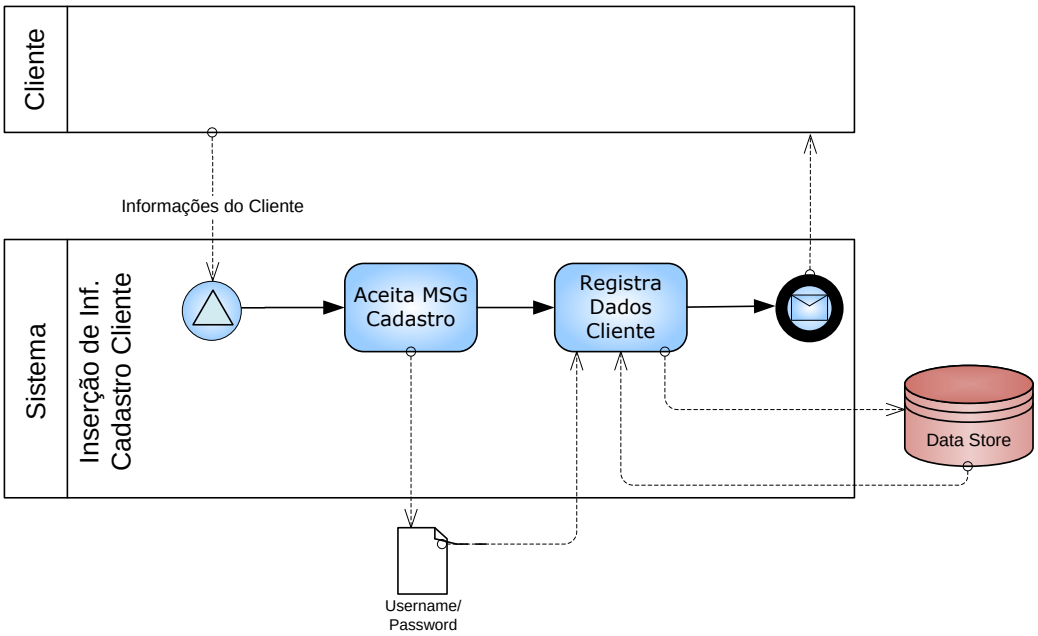


Figura 3 - Processo de Registro de Cliente

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.

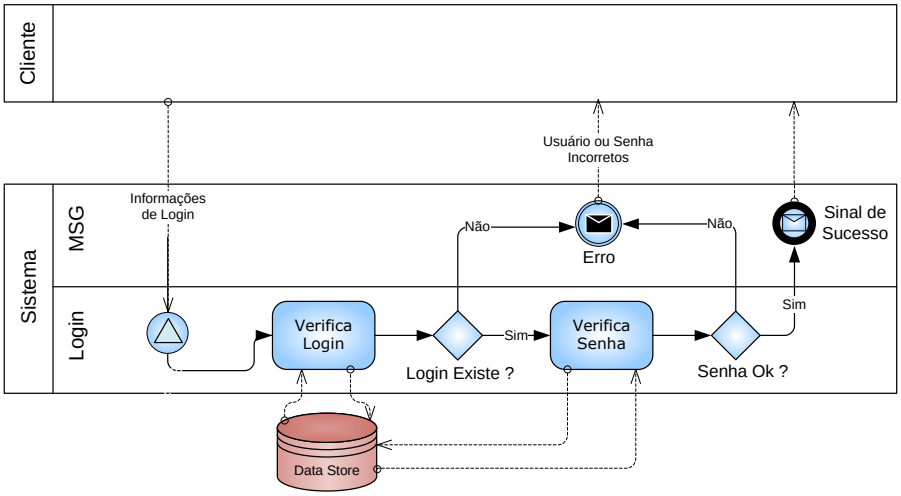


Figura 4 - Login no Sistema

Ao entrevistar o gestor do sistema, puderam ser evidenciadas questões óbvias. A combinação login / senha tem demandas de confidencialidade. Também há a demanda

de Confiabilidade[2] do sistema como um todo, visando proteger o negócio. Uma situação de ataque está ilustrada na figura 5.

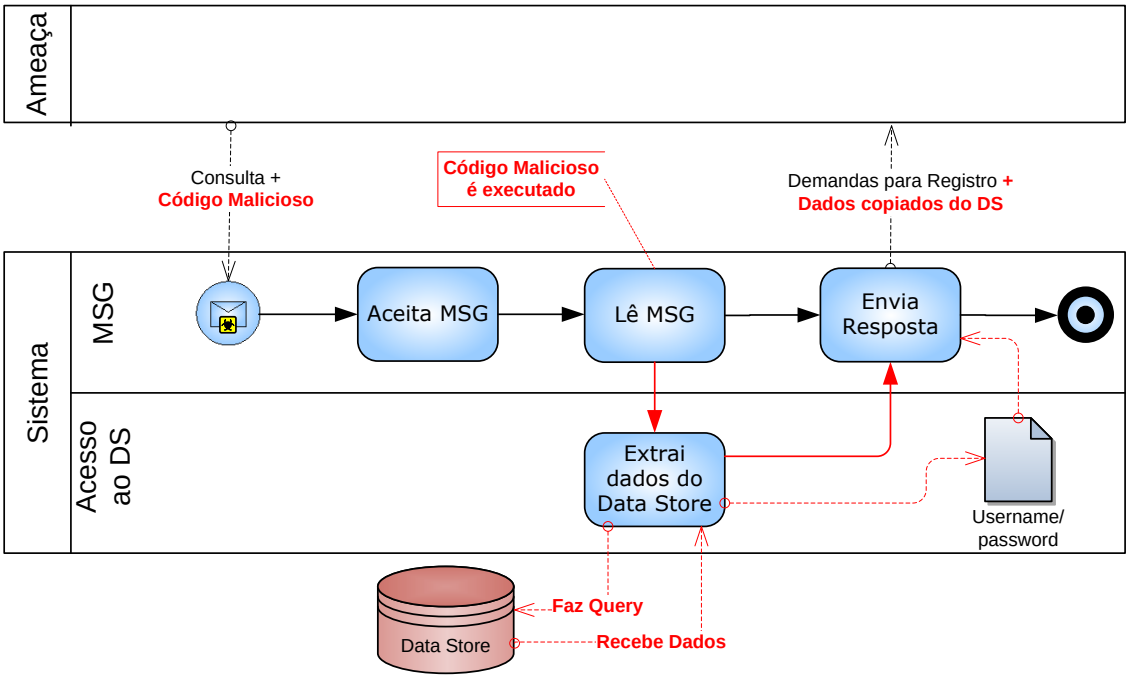


Figura 5 - Ataque ao Sistema

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/).

++

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.

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

Anexo do Case – 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 de riscos decorrentes dos tipos de incidentes sublinhados, devendo os mesmos serem tratados.

Template do Estudo de Caso

Nome: _____

Turma:_____ Data: _____

1. Critérios de Aceitação do Risco:

   _____

   _____

   _____

   _____

   _____

   Um critério de aceitação de risco é uma fronteira entre o aceitável e o inaceitável para o negócio. Limites financeiros, perda de *market-shar*e e comprometimento de metas são critérios típicos. Neste trabalho, vamos usar a abordagem QUALITATIVA, estabelecendo condições perceptíveis porém baseadas em condições limite não numéricas. Por exemplo, podemos definir que não são aceitos incidentes de segurança de forma a causar perda irreversível de clientes, a ponto de provocar comprometimento da imagem. Observe que este critério é abrangente, servindo para todos os setores da empresa, inclusive para o foco do trabalho que é a loja virtual. Leia o ANEXO do case antes.

2. Mapeamento dos Ativos mais Relevantes:

Ativo	Tipo	Fase	Informação Sensível
BD	F/T	A	Cadastros de clientes, estoque, preços

   _____

   _____

   _____

   _____

   O mapeamento de ativos é importante porque direciona as ações de treinamento, no caso de ativos humanos, favorece a utilização de auditorias produtivas, para processos ou sistemas, a permite o desenvolvimento de ações físicas onde o risco é maior. A coluna “Tipo” deve definir se o ativo é (F)ísico, (T)ecnológico ou (H)umano, ou uma combinação deles. A coluna “Fase” define se o ativo participa da (M)anipulação, (A)rmazenamento, (T)ransporte ou (D)escarte da informação, ou ainda uma combinação deles. Na coluna “Informação Sensível” vamos identificar qual ou quais informações efetivamente importantes para o negócio participam do alcance do ativo ora mapeado.

3. Mapeamento de Vulnerabilidades:

Vulnerabilidade	Ameaça	Possíveis Impactos
Código Vulnerável	Hacker	Roubo de Dados do BD

_____
_____
_____
_____

Mapear Riscos é a próxima fase, a partir da identificação das vulnerabilidades existentes no escopo em estudo. Vulnerabilidades são elementos passivos, como por exemplo funcionários destreinados ou com excesso de direitos de acesso aos sistemas e dados, equipamentos expostos ao acesso físico de estranhos ou bugs em sistemas que possam ser explorados interna ou externamente. Já a ameaça é um elemento ativo, que pode explorar a vulnerabilidade mapeada. Um concorrente pode convencer um funcionário desmotivado a roubar dados; um hacker pode explorar os bugs dos sistemas, e um elemento estranho, não necessariamente de forma intencional, pode danificar equipamentos que estejam expostos. O impacto é o resultado da ação da ameaça na vulnerabilidade.

4. Análise CIDAL:

	C	**I**	**D**	**A**	**L**
Ataque cibernético	**3**	**3**	**5**	**3**	**3**

Média: _____

Justificativas:

_____
_____
_____
_____

Na análise CIDAL, vamos agora avaliar um processo de negócio específico, em relação aos riscos evidenciados na fase anterior. Na segunda linha você

identificará o incidente da segunda linha da tabela do item 3 deste trabalho e na terceira linha trará o terceiro incidente escolhido. Para cada um deles você avaliará qual a intensidade do dado para o negócio, à luz do significado da tabela de métricas para o estudo de caso e do significado de cada atributo CIDAL. Atribua valores de acordo com a sua visão da extensão dos danos ao negócio para cada atributo. Ao final, calcule a média dos valores de CADA LINHA. Por exemplo, para a primeira linha do quadro, já preenchida como exemplo, a média é M1 = $\frac{3+3+5+3+3}{5}$ = 3,4. Calcule a média da segunda e da terceira linhas. Suponha que dê M2 = 2 e M3 = 4. Após isso, calcule a média das médias M = $\frac{M1+M2+M3}{3}$ = $\frac{3,4+2+4}{3}$ = 3,13. Este valor será usado no próximo passo.

5. Análise GUT:

Processo	Gravidade	Urgência	Tendência
Loja Virtual			

Resultado:

_____
_____
_____
_____
_____

Na análise GUT nós agregamos a urgência relativa em se restaurar cada processo afetado, quando submetido a um incidente. Um incêndio, por exemplo, demanda muito mais urgência na reação do que a perda de uma máquina, então deve ser priorizado. A Tendência agrega a antecipação de prioridade de um processo que talvez hoje não esteja com nível de sensibilidade alto, mas em função de planos e projetos estratégicos venha a se tornar mais sensível futuramente. Imagine uma empresa que está passando por um processo de fusão. Vários processos após a fusão ficarão mais sensíveis e outros talvez nem tanto. Para este trabalho considere que não há dados para análise de tendência, então vamos multiplicar por “1”, mas a urgência deve ser avaliada de acordo com a sua visão de agravamento do negócio com o passar do tempo em situação de impacto, multiplicando por “1” se você achar que há alta tolerância temporal, podendo a reação ser planejada sem pressa, “3” se a demanda por urgência é muito grande e “2” para uma situação intermediária. Na coluna GRAVIDADE você deve usar a tabela de conversão da página 57. Por exemplo, no CIDAL do exemplo tivemos um resultado final de “3,13” pontos, que na tabela de conversão está na faixa 2,4 ≤ C ≤ 3,7, que converte para “2”.

Os números da tabela GUT estão sempre entre 1 e 3 e o valor de cada célula deve ser multiplicado.

6. Avaliação do Risco e Tipo de Ação a tomar:

   _____
   _____
   _____
   _____
   _____

   Agora é a hora de usarmos o critério de aceitação de risco que definimos no item 1 deste trabalho. Se você achar que o risco é aceitável, bastarão apenas ações de controle do nível do risco. Escolha entre MODIFICAR, MANTER, ELIMINAR ou COMPARTILHAR. Se você considerar que o risco é INACEITÁVEL, além de indicar uma estratégia das 4 citadas acima, serão necessárias ações de Continuidade dos Negócios (um plano de contingências)

7. Esboço de DIRETRIZ de uma Política:

   _____
   _____
   _____
   _____
   _____

   DIRETRIZES são regras basais, cabíveis para qualquer colaborador, porém diretamente elaboradas para situações de risco evidenciadas durante o trabalho que fizemos. Identifique pontualmente um risco e descreva uma diretriz que servirá como uma regra para evitar que o incidente ocorra.

8. Ações de Continuidade dos Negócios:

   _____
   _____
   _____
   _____
   _____

   Aqui você pode escolher entre ações de Administração de Crise, de Continuidade Operacional ou de Recuperação de Desastre, indicando qual foi a que você escolheu e dando um exemplo. Não esqueça que ações de Administração de Crise envolvem comunicação com os *stakeholders*, de continuidade operacional são focadas no processo e não nos ativos, e de recuperação de desastres são focadas nos ativos, mas também nas lições aprendidas

Destaque estas duas folhas e entregue ao professor. Esta parte do trabalho valerá de 0 a 10 com peso 3 na nota final. Há uma cópia deste template em

http://www.fredsauer.com.br , caso fique acertado que o trabalho poderá ser enviado por e-mail.