UNIVER CIDADE

Pós-graduação em Projeto e Gerência de Redes de Computadores

Cadeira de Segurança da Informação
Prof.: Frederico Sauer, D.Sc.

Apresentação da Cadeira

O Curso é baseado na experiência diária do Prof. Frederico Sauer como Auditor de Segurança da Informação (certificado). O material didático adotado é o livro "Gestão da Segurança da Informação – Uma Visão Executiva", Ed. Campus, do Prof. Marcos Sêmola (FGV).

UNIVERCIDADE

Plano de Curso

- 48 horas de curso – 12 horas práticas

Data/turno	Atividade
12/01 manhã	Conceitos Gerais de SegInfo
19/01 manhã	Security Officer, PDS, Estudo de Caso
26/01 manhã	Plano de Continuidade, Estudo de Caso
26/01 tarde	Primeiro Lab – Uso de Ferramentas
09/02 manhã	Política de Segurança, Estudo de Caso, Análise Básica de Risco
16/02 manhã	Controles de Segurança, Ética e Forensics, Estudo de Caso
23/02 manhã	Criptografia, PKI e Segurança em Wireless, Análise de Riscos
23/02 tarde	Segundo Lab – Ferramentas de Apoio à Análise de Riscos

UNIVER CIDADE

Objetivos do Curso

- Capacitar o aluno a enfrentar os desafios impostos pela mudança de paradigma nas empresas, planejando, gerenciando e implementando técnicas de Gestão de Risco;
- Apresentar uma estratégia para integração das visões técnica e de negócios;
- Apresentar o conteúdo da ementa de uma forma gradativa e auto-contida em exposições de soluções que usem as tecnologias a discutir;
- Verificar requisitos básicos para a Gestão da Segurança da Informação nas empresas, focados nas normas em vigor;

A ênfase do curso é a associação das necessidades estratégicas dos processos de negócio da empresa a uma de suas componentes mais negligenciada, a SegInfo.

UNIVER CIDADE

Importância da SID nos tempos

Era	Ambiente	Material	Foco	Posição da SID
70 - 80	Mainframe	Dados	Disponibilidade	Apoio
80 - 90	Mainframes e Redes	Dados e Informações	Disponibilidade e Confidencialidade	Apoio, Administração e Operação
90 – 2K	Mainframes, Redes e Internets	Dados, Informações e Conhecimento	Disponibilidade, Confidencialidade, Autenticidade, Integridade e Legalidade	Negócio

UNIVER CIDADE

A Segurança é Importante ?

- Qual é o nosso nível de dependência ?
  - Quanto tempo podemos ficar sem nossos dados ?
  - Quanto tempo cada sistema pode ficar parado ?
- Qual é o nosso nível de sensibilidade ?
  - Pode ser útil para o seu concorrente ?
  - Pode ficar publicamente disponível ?
- Qual é o valor da sua reputação ?
  - Haverá dano em caso de modificações ou interrupções ?
- Quem pode se interessar por tudo isso ?
  - Agentes externos ? Internos ?
  - Há risco de caráter culposo ?

É raro nas empresas a presença de sensibilidade nos executivos quanto a importância da SegInfo. Na verdade, por cada um dos processos de negócio os dados, muitas vezes sigilosos e estrategicamente importantes, são manipulados, tramitados e destruídos, sem que procedimentos básicos sejam adotados. Um caso recente (FORD) nos mostra o quanto um simples descuido com a informação Digital pode causar de prejuízo para um projeto.

As questões acima, referentes aos dados da empresa, nos ajudam a refletir sobre a importância da manutenção da SegInfo para os nossos processos de negócio.

A questão, na verdade, gira em torno dos riscos aceitáveis para cada um dos processos de negócio, que inevitavelmente estarão presentes. A Segurança da Informação nada mais é do que uma ciência do campo da gestão de riscos. A missão do Security Officer, então, será exatamente manter esse risco permanentemente conhecido e sob controle. Para isso, inúmeras tarefas se fazem importantes, como por exemplo: conhecer, planejar, agir, auditar, educar, monitorar, aprender e gerenciar. As técnicas para se atingir esse objetivo serão apresentadas durante o curso.

UNIVER CIDADE

O que pode resolver o problema ?

- Compra de equipamentos e software de última geração ?
- Rígidas regras comportamentais com severas punições ?

Nenhuma atitude isolada obterá pleno êxito.

Segurança → Gestão de Riscos: Conhecer, Planejar, Agir, Auditar, Educar, Monitorar, Aprender, Gerenciar, etc.

A grande maioria das empresas confunde SegInfo com a compra de equipamentos e softwares caros e complexos (firewalls, IDS – Intrusion Detection Systems e antivírus). Outras imaginam que podem resolver suas fragilidades adotando Políticas de Segurança rígidas, com proibições e penalidades elevadas, mantendo uma equipe responsável por todo aparato tecnológico implementado. Isoladamente, nenhuma destas ou de outras providências obterá êxito, uma vez que a SegInfo possui componentes no campo físico, tecnológico e, principalmente humano, e que a fragilização de qualquer uma delas pode implicar em perdas, mesmo que as outras não estejam presentes.

UNIVER CIDADE

Segurança sem Metodologia

Esse é um exemplo ilustrado do que se disse anteriormente. Qual é o bem a ser protegido ? Como a informação em formato digital é facilmente manipulável em dispositivos diminutos, a complexidade é ainda maior.

UNIVERCIDADE

Importância da Informação

- Mais importante ativo – ganho de produtividade, redução de custos, obtenção de *market share*, apoio a tomada de decisão

Uma das frases mais ditas pelos teóricos da administração moderna é: "quem tem a informação tem o poder". As decisões hoje em dia são fundamentadas em dados estratégicos, pesquisas, e mais recentemente até em inferências realizadas através de *business inteligence*, onde técnicas de inteligência artificial (*data mining, clustering*, métodos estatísticos modernos, algoritmos genéticos e Redes Neurais) são aplicados aos processos de negócio para apoio à tomada de decisões.

Antigamente, a informação era privativa do topo da pirâmide da empresa, e mesmo com a informação inicial ela era centralizada devido às características típicas dos mainframes. Com os processos de *downsizing* e as primeiras Redes de Computadores, a informação passou a ser compartilhada, permitindo a implementação do *empowerment*, onde a informação está efetivamente disponível para todos os membros da empresa através de seus processos de negócio. Na verdade, os dados são o "combustível" destes processos, passando por todos eles e gerando as informações necessárias para a tomada de decisões em cada um dos níveis.

Visão Holística do Risco

- Cada empresa tem um universo próprio
- O nível de risco é crescente em virtude do crescimento da conectividade
- Assim como processos já comuns como o risco jurídico, risco de crédito, risco financeiro e pessoal, o risco da informação vem tomando importância nas corporações
- Ações corporativas integradas, com o emprego de mecanismos de controle buscam reduzir o risco a níveis aceitáveis

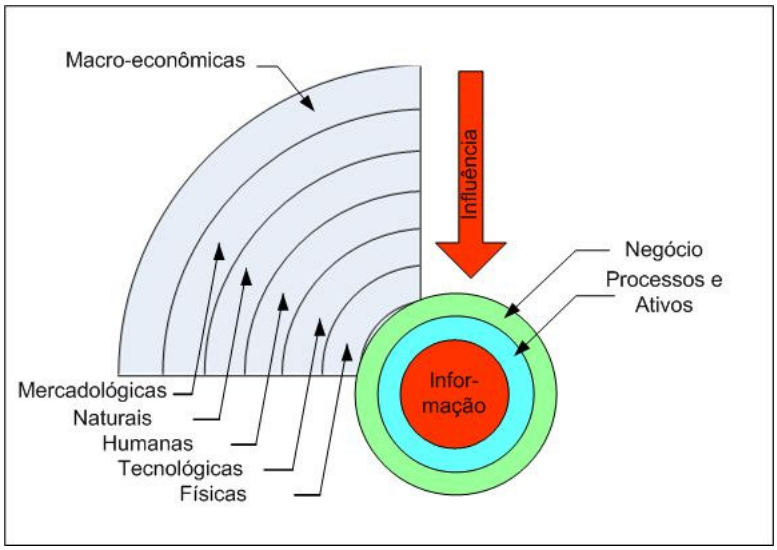
O grande problema nesse ambiente atual é que a Informação está mais vulnerável, uma vez que é manipulada por um número muito maior de pessoas, e muitas vezes, através dos processos modernos de B2B, B2G, B2C, ERP, etc, estão disponíveis também para elementos estranhos à organização corporativa proprietária da informação. Outro aspecto a ser levado em conta nesse cenário é que as empresas estão cada vez mais dependentes desta informação, cuja ausência ou perda de credibilidade pode afetar vários processos de negócio. Em muitos casos, a empresa é a informação (vide amazon, google).

É antiga a preocupação com vários tipos de riscos que as empresas correm, como o risco jurídico, financeiro e etc, mas hoje é cada vez mais presente a preocupação com o risco da informação.

Há alguns aspectos particulares a ressaltar: o primeiro deles é que cada empresa possui características próprias e não há uma estratégia padrão que possa ser adotada. O segundo diz respeito aos fatores externos que influenciam a sensibilidade que a empresa tem da informação. Apenas peculiarizando o problema de cada empresa uma estratégia global poderá obter êxito na tarefa de controlar o nível de risco. É por isso que o risco deve ser avaliado de forma holística, ou seja, é preciso avaliar o problema como um todo, não só quanto aos vários processos de negócio mas também quanto ao mundo externo que cerca a empresa.

UNIVERCIDADE

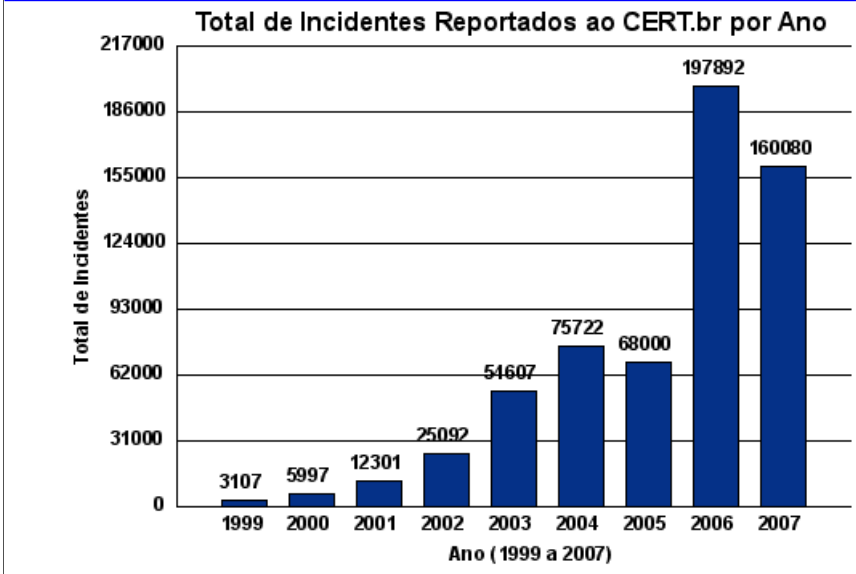
Influências que personalizam



Essa figura apresenta algumas variáveis externas que personalizam a gestão do risco, uma vez que influenciarão as componentes humana, tecnológica e físicas que cercam a informação da empresa através dos processos de negócio, e que provocarão variação no nível de sensibilidade da empresa.

UNIVER CIDADE

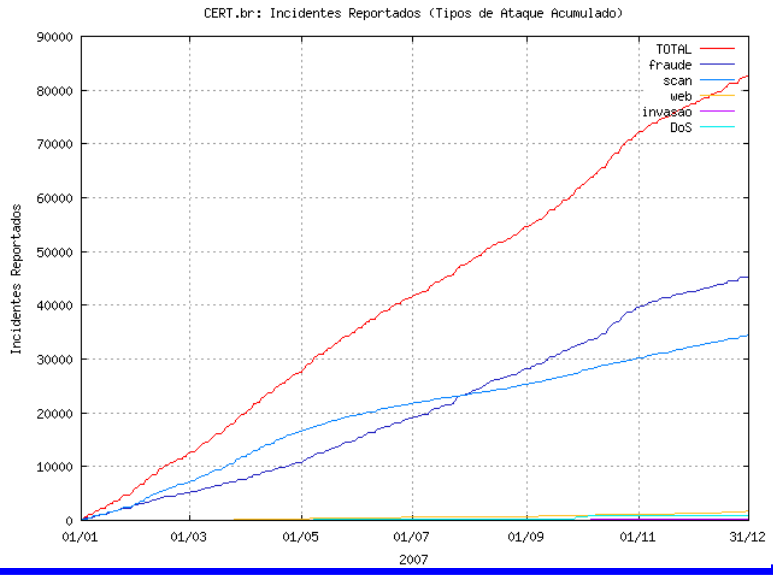
Será que há Ameaças ?



Os gráficos a seguir apresentam as estatísticas disponíveis no CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) para demonstrar o aumento dos incidentes de segurança, sendo que a fraude, incidente tipicamente motivado por questões econômicas/financeiras, tem sido o destaque.

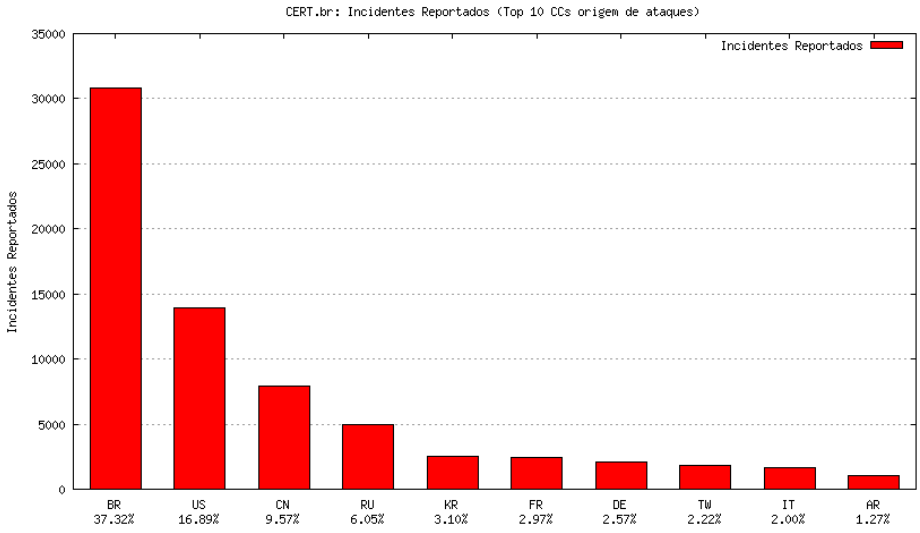
UNIVERCIDADE

Será que há Ameaças ?



UNIVERCIDADE

Será que há Ameaças ?

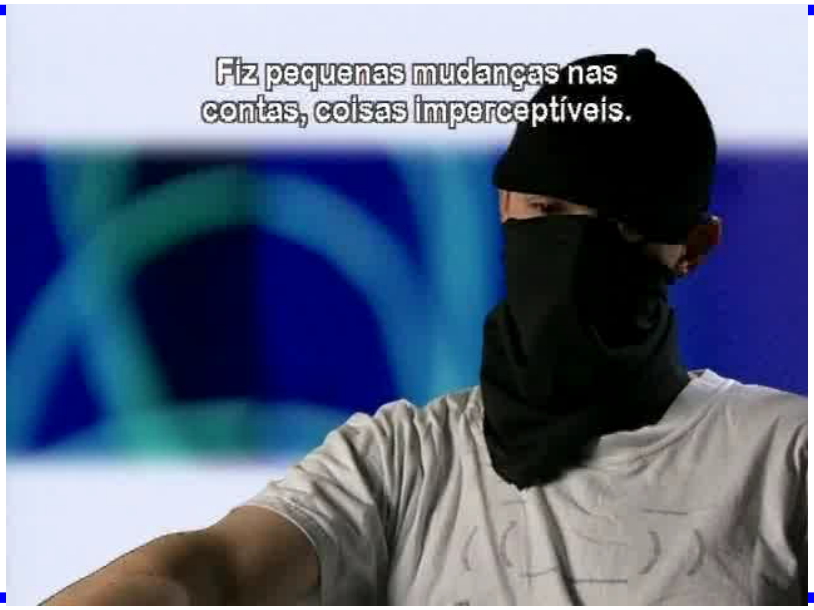


UNIVER CIDADE

Qual é a ameaça mais atuante ?

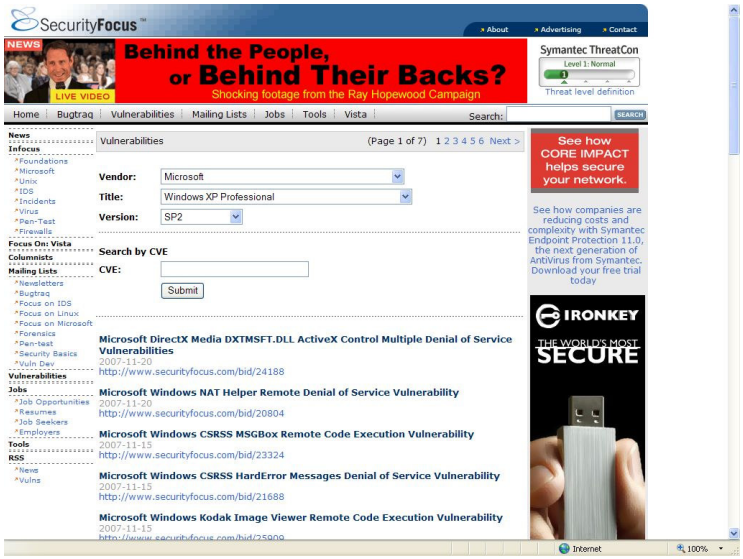
UNIVER CIDADE

Será que há Ameaças reais?



UNIVERCIDADE

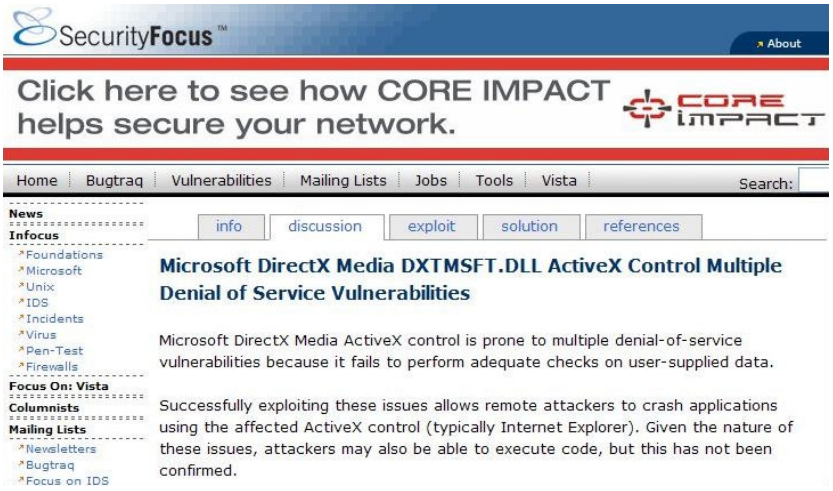
Será que existem vulnerabilidades ?



Essa é uma demonstração de uma vulnerabilidade descrita no site securityfocus, (www.securityfocus.com) que, entre outras coisas, divulga uma relação de vulnerabilidades descobertas nos sistemas operacionais e aplicações mais usadas mundo afora.

UNIVER CIDADE

Como elas podem ser usadas ?



UNIVERCIDADE

Será que existem *exploits* ?

SecurityFocus™ About

Download Encryption Tool
Disk & File Encryption Software for PC, Laptop, PDA and Mobile PC!
www.infotecs.biz
Ads by Google

Home | Bugtraq | Vulnerabilities | Mailing Lists | Jobs | Tools | Vista | Search:

News
Infocus
- Foundations
- Microsoft
- Unix
- IDS
- Incidents
- Virus
- Pen-Test
- Firewalls

Focus On: Vista
Columnists
Mailing Lists
- Newsletters
- Bugtraq
- Focus on IDS
- Focus on Linux
- Focus on Microsoft

info | discussion | exploit | solution | references

Microsoft DirectX Media DXTMSFT.DLL ActiveX Control Multiple Denial of Service Vulnerabilities

To exploit this issue, an attacker must entice an unsuspecting user to access a malicious webpage.

The following exploits are available:

- /data/vulnerabilities/exploits/24188.html
- /data/vulnerabilities/exploits/24188-2.html

Além da vulnerabilidade, diz como ela pode ser explorada...

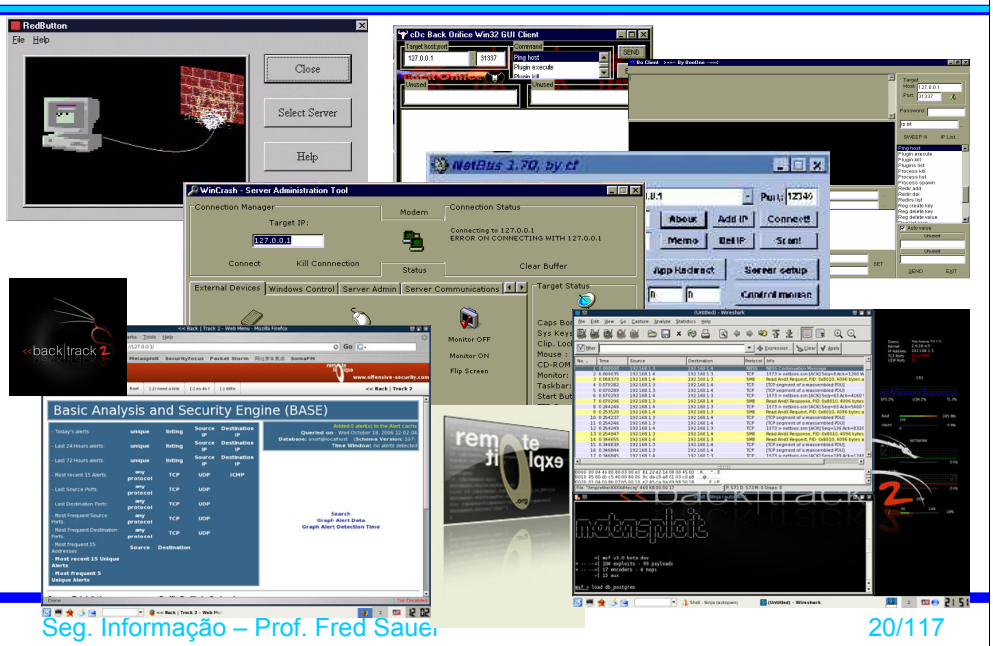
UNIVERCIDADE

Há cura ?

Obviamente, também disponibiliza a solução, caso a intenção do visitante seja resolver o problema, e não explorá-lo...

UNIVER CIDADE

Há Ferramentas de Ataque ?



Na Internet, são mais fáceis de se encontrar ferramentas de ataque do que soluções para vulnerabilidades, principalmente se falando do windows, que tem o código fechado. Apesar de se chamar genericamente de hacker todo aquele que invade sistemas, na maioria das vezes trata-se apenas de alguém que teve a paciência de ler um ou dois "*how-to*" e usou as ferramentas adequadas.

UNIVER CIDADE

Será que a ameaça é apenas externa ?

Essa figura apresenta a questão que também é típica nas empresas, de achar que as ameaças são exclusivamente externas, quando a grande maioria das vezes o inimigo é um usuário insatisfeito ou até mesmo mal-intencionado. Um dos membros da "família Noé" – o pica-pau, furando a arca que os conduz...

UNIVER CIDADE

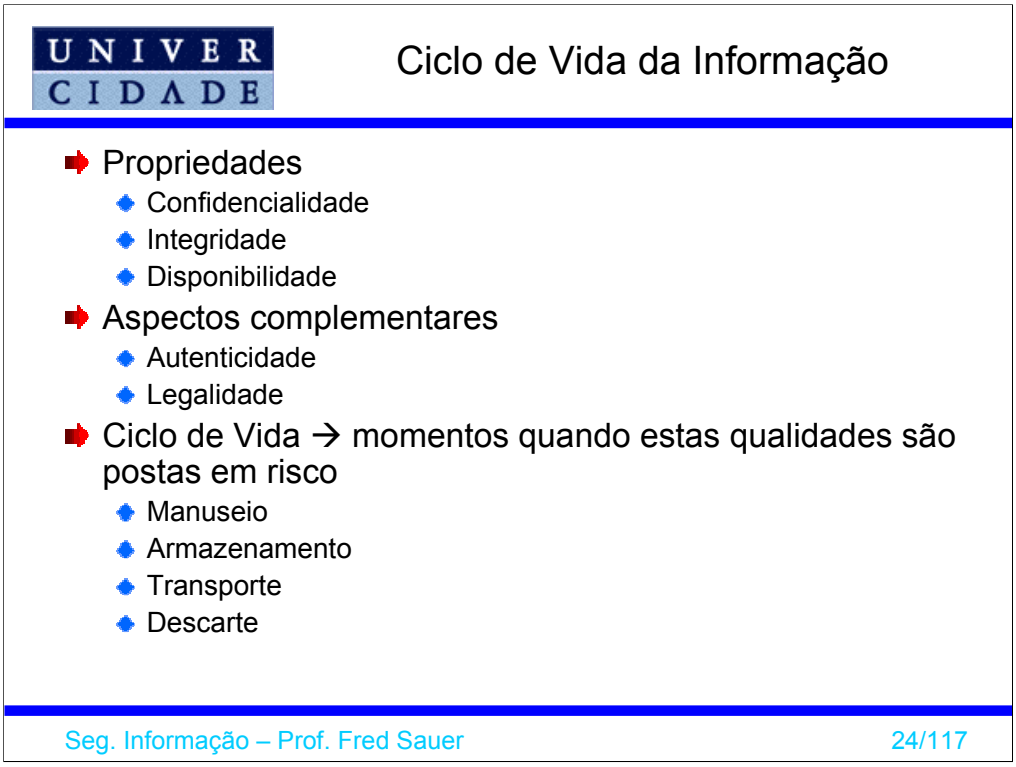
O que motiva uma ameaça a atacar ?

UNIVER CIDADE

As empresas estão percebendo isso ?

Seg. Informação – Prof. Fred Sauer 23/117

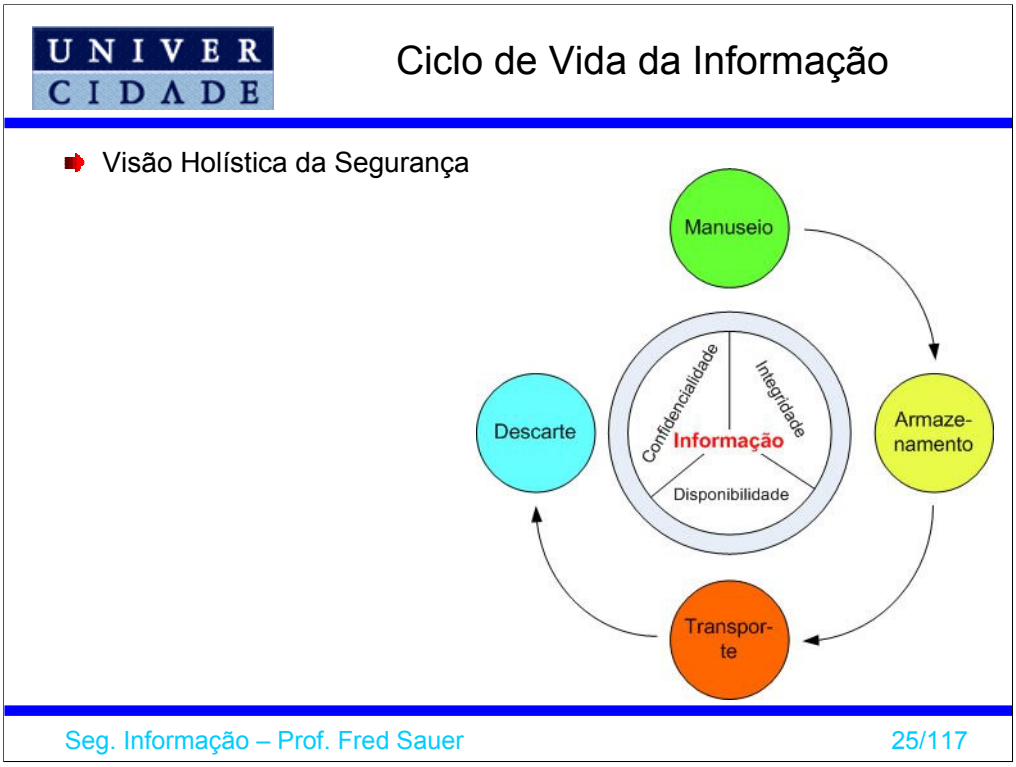
O HSBC foi o primeiro banco a encarar com naturalidade e objetividade o problema da segurança. Para os bancos, quanto mais usuários do sistema de banking pela Internet, melhor. A proposta da instituição é que, com medidas preventivas simples, as transações via internet são bastante seguras. Sua mais recente campanha publicitária mostra um personagem as voltas com várias ameaças, como o ladrão que despenca quando ele sente frio e resolve fechar a janela; a vizinha fofoqueira que tenta espiá-lo é nocauteada quando ele resolve jogar o lixo fora; no caminho, decide ligar o sistema de irrigação e destrói equipamentos de escuta clandestina posicionados no seu quintal. A mensagem é: com alguns cuidados básicos, a vida pode ser segura. O ladrão, a vizinha e o espião são as ameaças, como os vírus e hackers, a janela e porta fechada, bem como o sistema de irrigação seriam os mecanismos de segurança capazes de, apesar da total desatenção do personagem Haroldo, foram capazes de protegê-lo.



Após justificar a importância da informação para o negócio, é igualmente importante descrever que características devem ser preservadas na informação, de forma a considerá-la útil para o negócio. Três propriedades são consideradas principais, por serem primitivas. São elas: a confidencialidade (ou privacidade), que pode variar de acordo com o nível de sensibilidade da mesma, e do conjunto de elementos (pessoas) que devam conhecê-la. A integridade é uma propriedade que garante que a informação tem as mesmas características que tinha quando foi manipulada legalmente pela última vez. A disponibilidade permite que a informação possa ser usada sempre que necessária. Convém ressaltar que essas propriedades, apesar de isoladas, apenas tem valor se complementares. Por exemplo, não adianta uma informação estar disponível se a mesma não estiver íntegra, por exemplo.

Outros aspectos, complementares a estes três, hoje em dia se fazem necessários. São eles a autenticidade, que garante que a informação efetivamente foi criada ou manipulada por quem reivindica sua autoria. Um exemplo é o uso de uma senha de acesso. A legalidade permite garantir alguns aspectos interessantes. Um deles é a compatibilidade com as leis, regulamentos e normas que cercam o ambiente onde a mesma é utilizada. O outro aspecto atual é a não-repudiação de autoria, ou seja, mesmo que um usuário tente negar que realizou uma determinada transação qualquer que ele efetivamente tenha realizado, isso não seja possível através de algum mecanismo de comprovação com documentos digitais particulares. A autenticidade também contribui para a obtenção desta característica.

O ciclo de vida diz respeito a todos os momentos onde a informação é exposta a riscos, e agora já podemos dizer, de comprometimento de um ou mais aspectos de segurança citados acima. Estes momentos são vivenciados quando os ativos da empresa, sejam eles físicos, tecnológicos ou humanos, fazem uso da informação disponível, alimentando os processos de negócio e fazendo a empresa funcionar.



Há quatro momentos do ciclo de vida da informação quando a mesma é colocada em risco. São eles:

• Manuseio – envolve a criação e a manipulação da informação. O simples folhear de um maço de papéis ou a digitação de uma senha representa o manuseio da informação.

• Armazenamento – Trata-se do momento em que a informação é depositada em algum repositório, seja ele um banco de dados, um arquivo metálico ou em um disquete.

• Transporte – momento quando a informação trafega entre um repositório e outro, seja através de e-mail, fax, ou até mesmo através de uma linha telefônica.

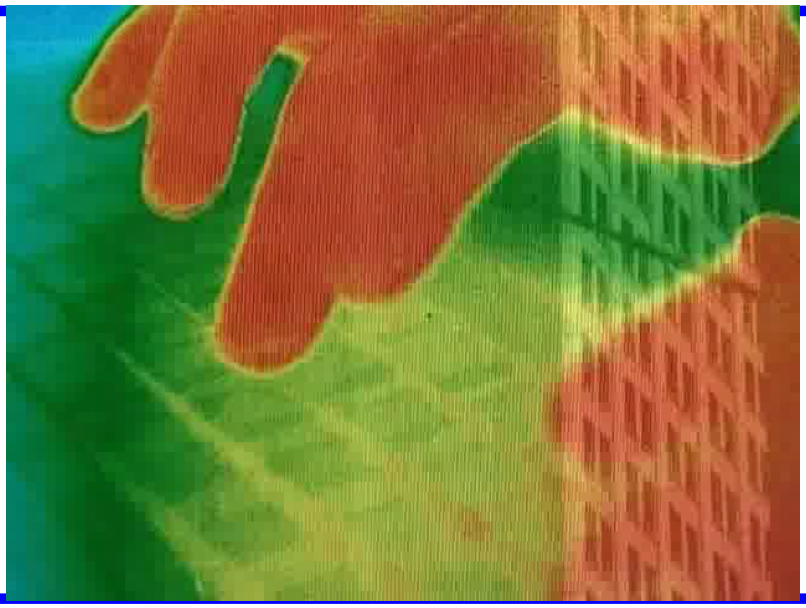
• Descarte – um dos mais negligenciados. Quem já não ouviu dizer que se conhece uma pessoa pelo seu lixo ? Essa fase diz respeito à deleção de uma informação, o descarte de um cartão de crédito, disquete ou CD que foi danificado, ou ainda o rascunho de um relatório confidencial que foi digitado.

Em cada um destes momentos as necessidades dos aspectos de segurança devem ser questionados e garantidos, quando necessário.

A segurança dele ser encarada de forma holística, ou seja, não adianta garantir apenas ALGUNS aspectos de segurança em ALGUMAS fases do ciclo de vida da informação, pois a mesma estará vulnerável aumentando o risco muitas vezes a um nível inaceitável. Precisamos agora definir que nível é esse.

UNIVER CIDADE

O descarte é importante ?



UNIVERCIDADE

Desafios

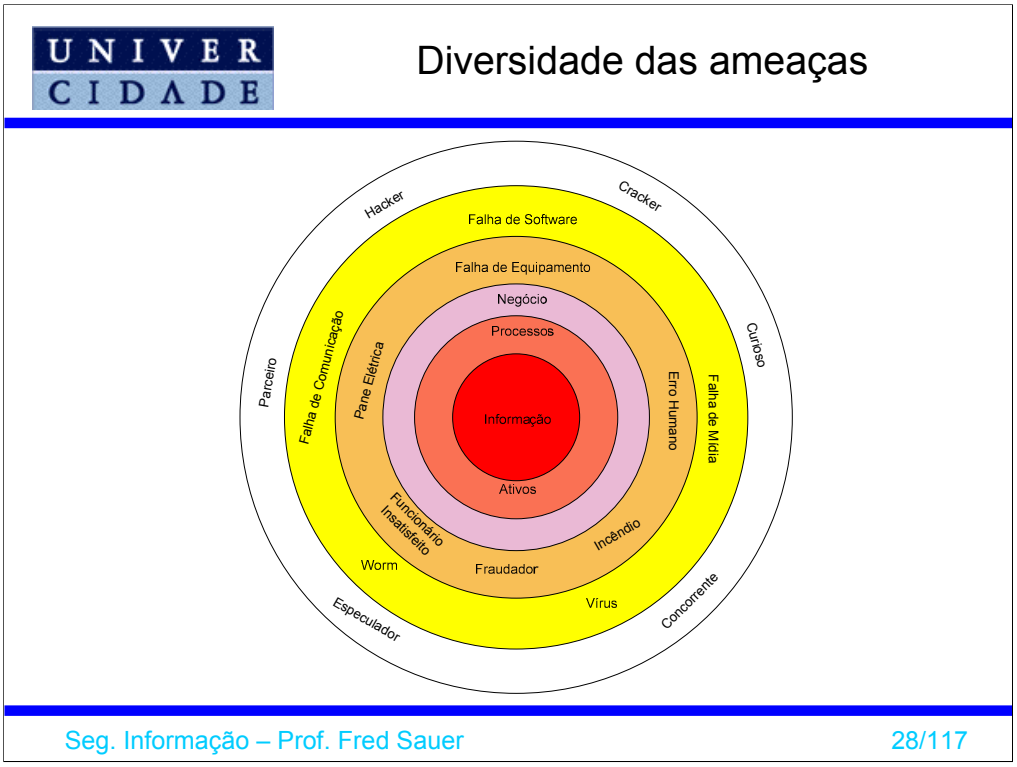
- Detalhar e segmentar o problema
- Percepção básica:
  - Alvo é a informação
  - A informação circula por toda a empresa
  - A informação é sensível a impactos
  - As vulnerabilidades transcendem o campo tecnológico, havendo riscos físicos e humanos
- Primeiro passo é identificar todos os elementos (ameaças) que interferem nos riscos
- É importante perceber que não há segurança absoluta e sempre haverá risco, que deve ser ajustado à natureza do negócio

Antes de propor uma solução para este problema, é preciso inicialmente definir O PROBLEMA, com detalhes suficientes para a construção de uma solução precisa. Outro aspecto é que, pela dimensão do problema, é importante que o mesmo seja segmentado de forma a permitir soluções customizadas.

Antes de mais nada, é importante perceber que a informação é onipresente, alimenta os processos de negócio e está sujeita a impactos específicos. Suas vulnerabilidades não são apenas tecnológicas, provocadas por falhas de projeto (como *bugs*), vírus, hackers e outros, mas também há aspectos físicos (como por exemplo a facilidade de acesso à mesma por pessoal não-autorizado) e humanos (como a manipulação inadequada da informação por pessoal que, apesar de possuir direitos de acesso, não possuem o treinamento adequado).

Os riscos que a empresa corre no que diz respeito aos aspectos de segurança da informação são influenciados por elementos internos e externos, que precisam ser identificados – é a anatomia do problema.

Esse ambiente interno e externo influenciador é profundamente dinâmico e sempre estará presente, de forma que é absolutamente impossível reduzir o risco a zero. Mas é possível controlar e monitorar esse nível de risco para níveis aceitáveis, de acordo com a natureza do negócio (dependência da informação para os processos de negócio).



Essa figura mostra a diversidade panorâmica das ameaças que expõe um negócio a riscos, e é fácil observar o seu dinamismo. Um funcionário insatisfeito, por exemplo, pode estar atuando de forma discreta e dissimulada, anos a fio sem que se perceba. Novos funcionários insatisfeitos podem surgir, após a descoberta e demissão do mesmo. Vírus atualmente são polimórficos e de difícil detecção. Concorrentes, hackers e outros terão maior ou menor interesse nas informações da empresa de acordo com o seu valor.

UNIVER CIDADE

Visão Corporativa

- Erros básicos do dia-a-dia são trazidos para a empresa
- Tipicamente, aspectos tecnológicos são privilegiados em detrimento aos físicos e humanos
- Investimentos são feitos à revelia de objetivos estratégicos e ações são reativas, e não orientadas por um Plano Diretor de Segurança

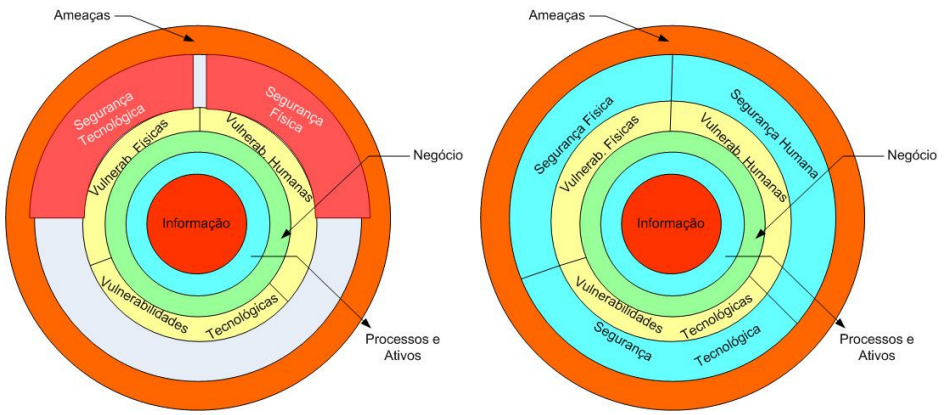
Pense agora na sua casa. Tipicamente, as residências possuem duas portas, uma social de outra de serviço, ambas para isolar o aconchegante e seguro ambiente interno da casa do hostil ambiente externo. Estas portas nada mais são do que dispositivos de segurança, e uma vez que o valor a proteger, seus bens, sua família, estão acessíveis através de qualquer uma das duas portas, ambas deveriam possuir os mesmos recursos de segurança, como trancas, alarmes, etc, para distribuir os investimentos e oferecer um único nível de segurança para um único bem a proteger. É isso que acontece ???

Outro aspecto relevante é que preocupa-se muito com a implementação de mecanismos que muitas vezes não sabemos usar corretamente, e acabamos por não utilizá-los.

Há uma tendência de trazermos esses pequenos erros do nosso dia-a-dia para as nossas empresas. Os investimentos em segurança não possuem objetivos bem definidos nem são associados com os objetivos da empresa, ou seja, não estão ligados a nenhum estudo de ROI (Retorno sobre o Investimento). No caso específico da segurança, a elaboração de um Plano Diretor é fundamental para evitar gastos inúteis com segurança.

UNIVERCIDADE

Cenário atual x desejado

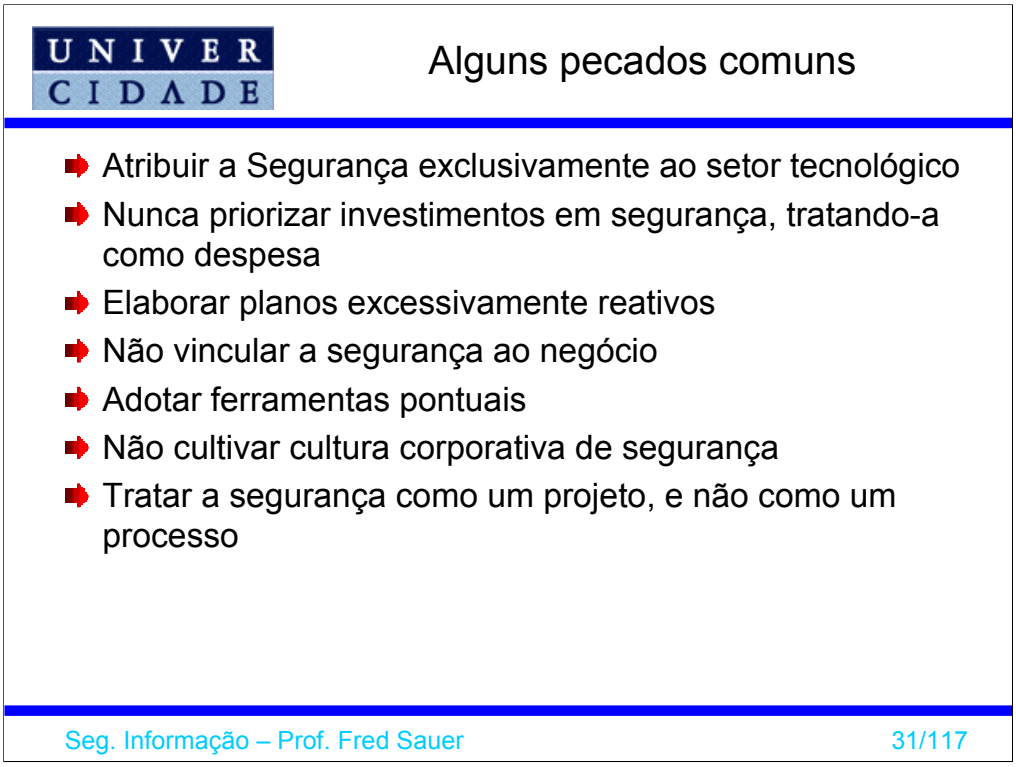


Seg. Informação – Prof. Fred Sauer 30/117

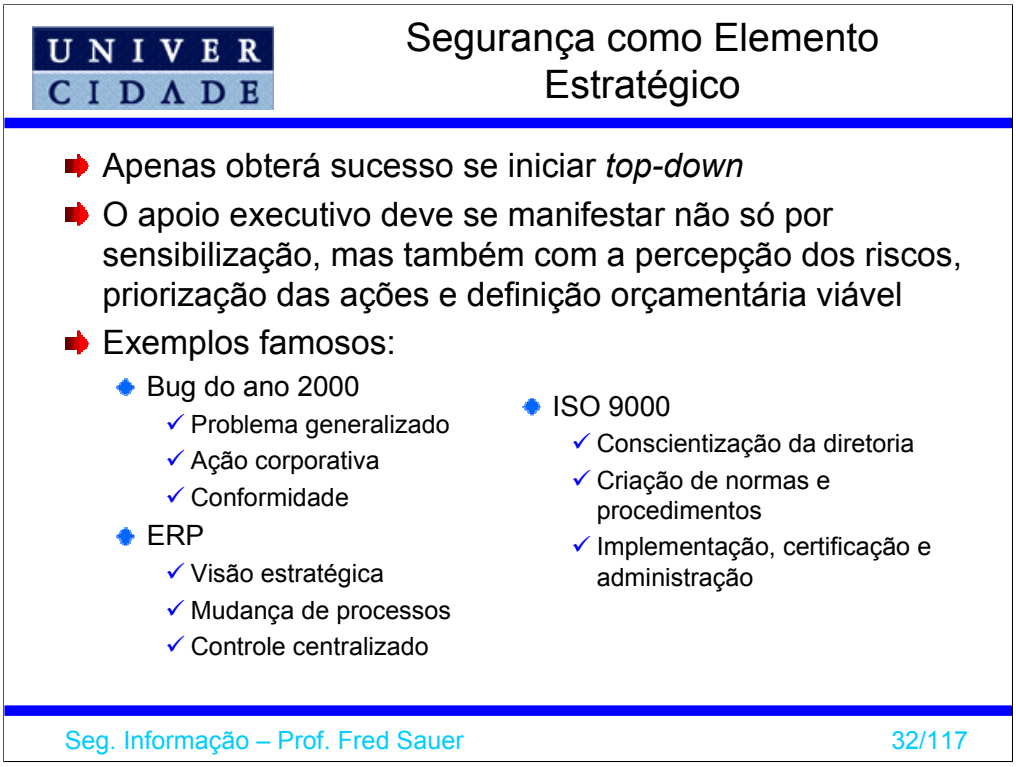
Atualmente, o que se observa é uma visão míope do problema da segurança, focando apenas em alguns aspectos e descuidando-se de outros. É como se enchêssemos apenas três pneus do carro para fazermos uma longa viagem.

A figura da direita apresenta a Visão corporativa Integrada desejada.

Convém também ressaltar que as vulnerabilidades e as ameaças desenvolvem uma relação simbiótica. As vulnerabilidades são intrínsecas ao nosso ambiente tecnológico (como falhas de Sistema Operacional), Físicas (como facilidades excessivas de acesso ao *datacenter* ou a falta de dispositivos de detecção de pessoas ao mesmo) ou ainda humanas (como momentos de descuido com precauções básicas de segurança do próprio funcionário da empresa). A relação entre as ameaças (agentes que exploram estas vulnerabilidades) com as vulnerabilidades é oportunista, ou seja, as ameaças buscam pontos fracos capazes de serem explorados. Um exemplo típico disso é a Engenharia Social, quando um elemento interessado nos dados de uma empresa obtém, através da conquista da simpatia e confiança de um elemento que conhece as "chaves" de acesso à informação, para obtê-las.



Acredita-se, na maioria das empresas, que a simples instalação de um bom *firewall* resolverá o problema da segurança. Não criam uma equipe especialista no assunto, delegando a responsabilidade pela SegInfo ao pessoal do desenvolvimento ou Suporte. O custo da segurança é desassociado do valor da informação, ou dos impactos de um eventual comprometimento da mesma, sendo então relegado a segundo plano. A gerência pró-ativa é rara, de forma que só se percebe a necessidade de um sistema eficiente contra vírus, por exemplo, depois da máquina ser contaminada e precisar ser formatada. Não há conhecimento e utilização de técnicas para associar a segurança aos processos de negócio. As ferramentas utilizadas não são integradas e monitoradas, por exemplo apenas algumas estações da rede usam antivírus, outras não. O aspecto humano é muito pouco privilegiado, de forma que não se desenvolve uma cultura corporativa em torno da segurança. Trata-se a segurança como um projeto a ser implementado e concluído, o que não é possível.



Uma das questões fundamentais no processo de gestão de risco é o comprometimento da alta administração da empresa. Se os executivos conhecerem os riscos e seus eventuais impactos para o negócio, é possível a implementação de ações coordenadas e eficazes. Ao contrário, como é realizado na maioria das vezes, se o processo for exclusivamente conduzido e imposto pela área tecnológica, não haverá sinergia suficiente para atingir resultados. Uma conseqüência óbvia é que não se conseguirá prioridade na obtenção de investimentos para treinamento, aquisição de ferramentas e implementação de perímetros de segurança, além de que eventuais proibições e imposições de limites serem desmoralizados por serem descumpridos principalmente pela alta cúpula da empresa.

Na história empresarial há alguns exemplos importantes que denotam a importância de processos top-down. A ISO 9000 é um dos melhores, quando os executivos observaram que se a empresa não obtivesse o nível de qualidade necessário para disputa de mercado, teriam perdas consideradas. Apesar de não ser um processo barato, é hoje um processo presente na grande maioria das empresas.

Um aspecto interessante a ressaltar é que nestes 3 exemplos acima, nove pontos foram destacados para ações distintas, porém que são igualmente importantes e pertinentes para a superação do desafio da Segurança da Informação nas empresas. Todos são fatores críticos da sucesso da SegInfo.

UNIVER CIDADE

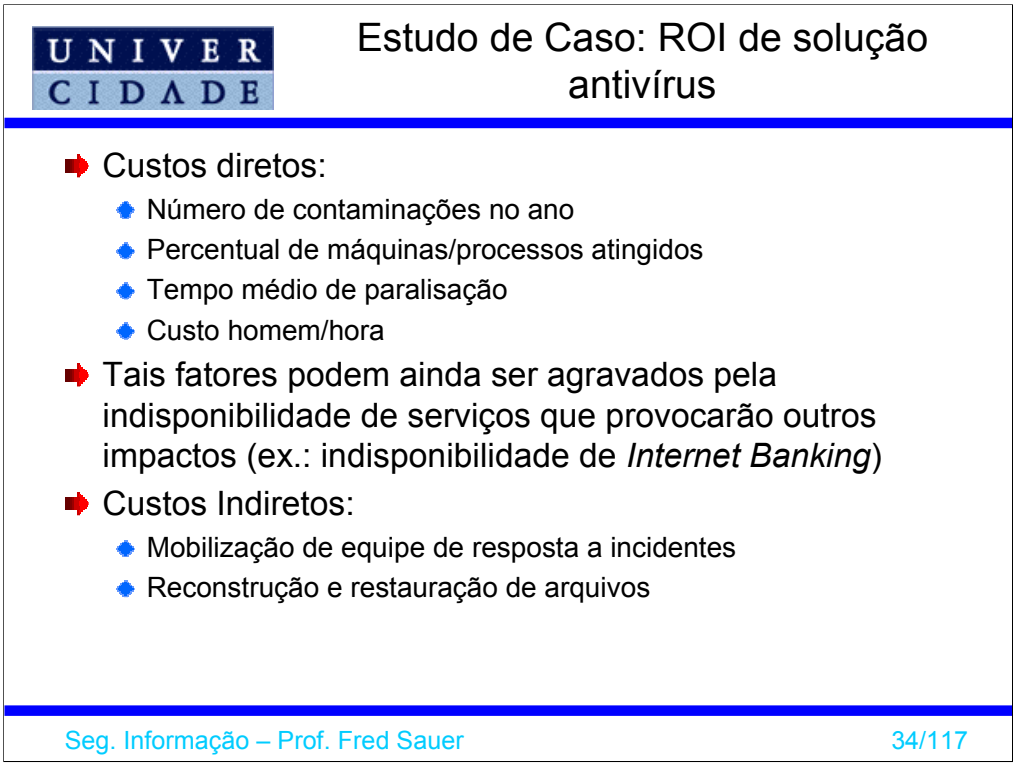
Retorno Sobre o Investimento

- Dialeto do empreendedor
- Cruza dados reais dos custos diretos, indiretos e intangíveis, com a projeção de investimentos
- Não há um modelo único e consagrado, mas a pergunta sempre é: devo realizar este investimento ?
- A dificuldade deste trabalho é construir o ROI com uma visão essencialmente corporativa

O ROI é uma ferramenta indispensável para empreendedores, investidores e executivos atentos ao mercado e sua oportunidades. Através do cruzamento de dados reais referentes a custos diretos indiretos e, principalmente intangíveis (a aí entra a sensibilidade do analista) com a projeção dos investimentos necessários para a implementação de alguma ação, pode-se subsidiar a tomada de decisão. Há vários modelos de ROI na literatura, e não há um modelo certo ou errado. O que diferencia um do outro é exatamente a profundidade da análise do problema.

Apesar de parecer estranho para os executivos, é uma ferramenta aplicável à área tecnológica, porém um pouco mais complexa de ser construída uma vez que sua principal componente de retorno é a intangível. E o principal retorno não é traduzido em lucro (benefício) e sim ausência de prejuízo.

Para possibilitar essa visão da tecnologia integrada ao negócio, é fundamental entender, conhecer e mapear os problemas corporativos, no nosso caso específico na área de segurança, para que essa análise possa ser precisa e o ROI possa ser construído.



Este é um estudo de caso baseado na experiência do professor com uma solução antivírus. A natureza do negócio nada tinha a ver com tecnologia, pelo menos a computacional. O primeiro passo é a coleta da dados relacionados com os custos diretos, indiretos e intangíveis associados a um eventual comprometimento da segurança ocorrido pela indisponibilidade de uma solução adequada. Neste momento, contabilizam-se todos os hh e eventuais ferramentas necessárias para solução pontual de um problema, e pode ser feito com base em uma suposição ou através de dados reais.

Há outros custos indiretos passíveis de contabilização não citados aqui, por estarem diretamente relacionados com o exemplo da contaminação por vírus. O custo do aumento de banda pelo uso indiscriminado do acesso à Internet (não relacionado com os objetivos no negócio), que demandará upgrades de link e conseqüentemente custo. Outros exemplos são sanções legais pelo uso de cópias não-autorizadas de software e roubos de informações sigilosas para venda a concorrente.

Estudo de Caso: ROI de solução antivírus

- Custos Intangíveis:
  - Houve comprometimento de informação sigilosa ?
  - Qual foi o impacto para a imagem da empresa ?
  - Qual é o custo para reconstruir a imagem de credibilidade da empresa ?
- O monitoramento constante é vital para novos investimentos em segurança → subsidia o ROI

A contabilização do intangível é a parte mais dependente do conhecimento do negócio, e a mais importante também, uma vez que são os fatores que efetivamente colocam em risco a continuidade do negócio. Pode ser traduzido em um impacto à imagem da empresa, cuja reconstrução pode demandar muito mais gastos do que foi gasto para construí-la. É o exemplo das "telas azuis" do *windows*.

Como se pode observar, para a construção de um ROI é vital que se possua mecanismos de controle para reunir informações que sinalizem eventos onde há quebra de segurança e registrem seus efeitos ao longo do tempo. Com estes dados, acrescidos de projeções e simulações especialistas, é possível a geração de um ROI que diga exatamente o que se pretende sobre a Segurança da Informação: que ela é um investimento importante, necessária, mensurável e justificável, e principalmente que ela traz efetivamente o retorno para justificar estes investimentos.

Estudo de Caso: ROI de solução antivírus

- Caso RM: solução para minimizar os impactos de epidemias virais
- Dados históricos (resumo)
  - Caso *Blaster*: aproximadamente 70% das estações críticas contaminadas
  - Tempo de quarentena para liberação final: 48 horas
  - Total de h/h comprometido (paralisado ou envolvido na recuperação): 3248 h/h
  - Impacto direto: R$ 142.912,00
  - Pressão dos clientes por cumprimento de cronogramas
  - Impacto subjetivo: A imagem de uma empresa vulnerável

Resumo de um estudo de caso real.

UNIVERCIDADE

Estudo de Caso: ROI de solução antivírus

- Solução analisada e homologada pela equipe técnica: *Policy Orchestrator*
  - Custo do investimento:
    - ✓ Contrato corporativo – valor subsidiado e suporte diferenciado
    - ✓ Custo do servidor mais estações: R$ 25.716,85 por dois anos
  - Conclusão:
    - ✓ Investimento obviamente vantajoso

Modelo de Gestão

- Formalização através das etapas:
  - Comitê Corporativo de Segurança
  - Mapeamento de Segurança
  - Estratégia de Segurança
  - Planejamento de Segurança
  - Implementação de Segurança
  - Administração de Segurança
  - Segurança na Cadeia Produtiva
- Conjunto de Processos Integrados, com um único objetivo: gerir dinamicamente controles abrangentes (processos, tecnologia e pessoas) operando sob risco controlado
- Evita investimentos redundantes, esforços contrários e possibilita a canalização da energia para o business da empresa

O mais importante a vislumbrar é que a segurança seja um processo dentro da empresa, e não um projeto; que as ações sejam coordenadas e que as variáveis deste processo estejam permanentemente ajustadas às diretrizes estratégicas do negócio. Mais uma vez citando, é um processo de gestão de riscos que são variáveis de acordo com as várias ações da empresa, não necessariamente ligadas à área tecnológica. Um processo de contratação de pessoal, por exemplo, aumenta o nível de risco por estar introduzindo no ambiente da empresa novos elementos humanos que passarão a ter acesso a informações da empresa, e que possuem visões diferentes da já implementada. Essa ação, por exemplo, precisaria ser acompanhada de ações de SegInfo para redução do risco operacional.

Não basta criar um elemento administrativo e delegar competências. Deve-se mapear os processos através das várias etapas do desafio corporativo da SegInfo, que são as citadas no slide.

Comitê Corporativo – Coordenar ações, medir índices de desempenho e reparar desvios de foco.

Mapeamento de segurança – Mapear processos de negócio, perímetros, ativos, ameaças, vulnerabilidades, impactos, necessidades em cada fase do ciclo de vida.

Estratégia de Segurança – Definir plano de ação plurianual com base nos subsídios acima, e principalmente criar sinergias, buscar comprometimento dos executivos através da sintonia do processo de SegInfo com às suas expectativas no negócio e, si.

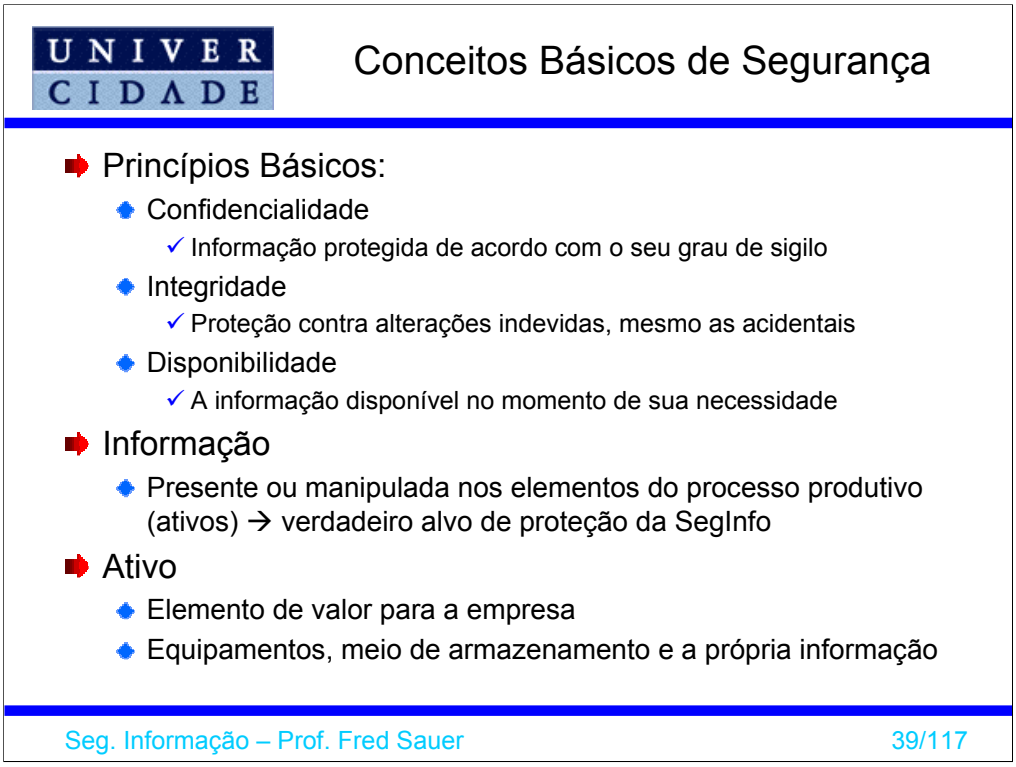
Planejamento de Segurança – Organização de vetores interdepartamentais, ações de capacitação (comprometimento com os objetivos), elaborar uma Política de Segurança.

Implementação da segurança – Divulgar permanentemente a política de segurança, ações detalhadas de capacitação para o ciclo de vida, implementação de mecanismos de controles físicos, tecnológicos e humanos para controle do risco.

Administração de segurança – Monitorar os controles, projetar o ROI, garantir a conformidade com as normas, manter planos de continuidade do negócio

Segurança na Cadeia Produtiva – Introduzir efetivamente a seginfo no negócio, envolvendo parceiros, fornecedores, clientes, governo, etc.

Essa gestão integrada é exatamente um dos benefícios tangíveis mais relevantes da implementação de ações de SegInfo, por permitir que não se façam ações desencontradas, conflitantes ou inúteis, e principalmente por associar essas ações ao business da empresa.



A implementação das ações de segurança são norteadas pelo objetivo da preservação dos atributos confidencialidade, integridade e disponibilidade durante todo o seu ciclo de vida.

A informação é o combustível dos ativos da corporação. Sem ela, as decisões não podem ser tomadas. Por conta disso, esses ativos é que são o verdadeiro alvo da segurança da informação, ou seja, o negócio em si.

O ativo é um elemento de valor para um indivíduo ou para uma organização, que por essa razão precisa de proteção adequada. Esses ativos compõe os processos que manipulam e processam a informação. Os ativos, para serem tratados de forma adequada, devem ser divididos e agrupados para melhor identificação de suas fronteiras. Com a definição destes grupos, pode-se tratar com mais especificidade e melhor avaliação qualitativa das ações de segurança pertinentes. Na área de SegInfo, a forma mais usual da identificação dos ativos envolve equipamentos, aplicações, usuários, ambientes, informações e processos. Mas nada impede que outros ativos sejam identificados de acordo com as particularidades do negócio de sua empresa.

UNIVER CIDADE

Conceitos Básicos de Segurança

- Aspectos da Prática da Segurança
  - Autenticação
    - ✓ Reconhecimento formal de uma identidade
  - Legalidade
    - ✓ Contratos, legislação e normas vigentes
- Aspectos Associados
  - Autorização
    - ✓ Permissão de acesso
  - Auditoria
    - ✓ Coleta de evidências
  - Autenticidade
    - ✓ Garantir identidade, autoria, originalidade, integridade e não-repudiação
  - Severidade
    - ✓ Gravidade do dano
  - Criticidade
    - ✓ Impacto ao negócio pela ausência de um ativo

Associados e complementares aos atributos Confidencialidade, Integridade e Disponibilidade, os elementos Autenticação e Legalidade, já citados anteriormente, são essenciais para a prática da SegInfo.

Para a busca destes atributos, alguns aspectos são especificamente importantes para sua avaliação:

Autorização – concessão de permissões para acesso à informações e aplicações que as manipulem. É concedida após a correta identificação e autenticação do usuário ou processo que pretenda acessar a informação, e é dependente de corretos controles de acesso precisamente definidos, como por exemplo a definição de direitos em áreas de dados de servidores, de acordo com o respectivo *logon*.

Auditoria – Coleta de evidências de uso dos recursos para acesso à informação, bem como o tipo de manipulação envolvida. Um exemplo é o log de acesso tipicamente implementado por Sistemas Operacionais e Sistemas Gerenciadores de Bancos de Dados.

Autenticidade – Garantia que a autoria de qualquer transação é autentica, ou seja, está ou foi realizada por quem se credenciou a fazê-la. Hoje em dia há recursos criptológicos como as assinaturas digitais que possibilitam um grau de autenticidade digital semelhante aos obtidos através de métodos físicos tradicionais.

Severidade – Caso uma ameaça explore uma vulnerabilidade, um ativo poderá sofrer danos que serão dimensionados de acordo com a gravidade deste dano para o negócio.

Criticidade – A redução ou a perda de algumas funcionalidades, podendo chegar até mesmo à perda total da disponibilidade de um ativo provocará naturalmente um impacto ao negócio, cuja gravidade será dimensionada como criticidade do evento.

UNIVER CIDADE

Conceitos Básicos de Segurança

- Ameaças
  - Naturais, voluntárias ou involuntárias
- Vulnerabilidades
  - Fragilidade efetivamente existente e que, se explorada, pode afetar um ou mais dos aspectos da Segurança
  - São elementos passivos
  - Podem ser:
    - ✓ Físicas
    - ✓ Naturais
    - ✓ Hardware
    - ✓ Software
    - ✓ Mídia
    - ✓ Comunicação
    - ✓ Humanas
  - Há uma relação oportunista entre as ameaças e as vulnerabilidades

As ameaças, que são personificadas em agentes ou condições que efetivamente causem incidentes que possam comprometer informações e os ativos a ela relacionados, através da exploração de vulnerabilidades existentes, são chamados de ameaças. Estas ameaças provocam impactos ao negócio, através do comprometimento dos atributos confidencialidade, integridade e disponibilidade. É importante destacar que estas ameaças tipicamente se utilizam de ferramentas disponíveis, que não são, por si só, ameaças. Um exemplo são os *exploits* para vulnerabilidades em um Sistema Operacional. A ameaça é o invasor, e não o *exploit*. Estas ameaças podem ser naturais, ou seja, provocadas por fenômenos da natureza, como incêndios, enchentes, etc. As Involuntárias são causadas quase sempre por desconhecimento ou descuido, como acidentes, erros, falta de energia, etc. As voluntárias, por sua vez, são propositais e causadas por agentes humanos que tem a intenção premeditada de criar um incidente de segurança.

As vulnerabilidades, elementos infelizmente sempre presentes nos ambientes computacionais, estão presentes ou associados a ativos que manipulam informações, e que podem ser objetivamente exploradas por ameaças, conscientemente ou não, causando incidentes de segurança que comprometam um ou mais aspectos da SegInfo (Confidencialidade, Integridade e Disponibilidade). A vulnerabilidade, por si só, não causa dano algum, ou seja, são elementos eminentemente passivos. Um exemplo disso é quando instalamos um Sistema operacional no nosso computador e iniciamos imediatamente a usar aplicações como browsing, e-mail, etc. O Sistema Operacional possui várias falhas que são corrigidas através de patches de segurança disponíveis no site do fornecedor, e devem ser instaladas para reduzir uo número de vulnerabilidades. Não ter instalado um firewall pessoal e um antivírus também aumentou bastante o índice de vulnerabilidade desse sistema em particular.

As vulnerabilidades podem ser:

• Físicas – falta de extintores, sensores de fumaça, riscos de acesso indevido, vazamentos, etc.

• Naturais – alta umidade, poeira excessiva, calor excessivo, etc.

• Hardware – desgaste, obsolescência, erros de instalação, etc.

• Software – Erros de configuração permitindo acessos indevidos, etc.

• Mídias – Sensíveis a radiação eletromagnética, etc.

• Comunicação – Perda de comunicação em rede, etc.

• Humanas – Mais presente a todas as instalações. Falta de treinamento de funcionários, não cumprimento de precauções básicas de segurança, sabotagens, vandalismo, roubo, invasões, etc.

UNIVER CIDADE

Conceitos Básicos de Segurança

- Medidas de Segurança
  - Preventivas
    - ✓ Evitar a ocorrência de incidentes
    - ✓ Políticas de Segurança, ferramentas (*firewall*, antivírus, etc.), palestras, etc.
  - De Detecção
    - ✓ Identificação de ameaças potenciais
    - ✓ Análise de Riscos, IDS, alertas, câmeras, alarmes
  - Corretivas
    - ✓ Equipe de Resposta a Incidentes, Plano de Recuperação de Desastres, Plano de Backup
  - Preditivas
    - ✓ Ligadas a eventos com alta probabilidade de ataques
  - Um Plano de Continuidade dos Negócios abrange medidas de todos os tipos
  - A validade dessa classificação é permitir planejar e focar as ações

É claro que existem práticas que buscam reduzir o nível de risco existente. São tipicamente medidas genéricas e corporativas, não direcionadas para um evento em especial, e sim para um conjunto de eventos com ocorrência intempestiva e de gravidade variável. Buscam sempre a proteção dos ativos através da proteção dos atributos de SegInfo. Tentam impedir que as ameaças explorem vulnerabilidades, reduzir estas vulnerabilidades, ou pelo menos reduzir o impacto causado por uma exploração com sucesso. O objetivo é sempre reduzir o nível de risco. São efetivamente controles desse nível de risco, e podem ter as seguintes características:

• **Preventivas** – Visam evitar que incidentes ocorram. Investem especialmente no ativo humano, e mesmo as ações tecnológicas e físicas dependem do fator humano para terem sua eficiência intensificada. São exemplos as ferramentas de controle de acessos e vírus, e as regras de segurança corporativa, que devem ser intensamente divulgadas e discutidas até que haja uma mentalidade corporativa de segurança.

• **Detectáveis** – São destinadas a identificar potenciais ameaças para que, através de sua monitoração permanente, possa se evitar que vulnerabilidades sejam exploradas. São exemplos as análises de riscos, IDS (Intrusion Detection Systems), câmeras de vigilância, alarmes de acessos indevidos, etc.

• **Corretivas** – Uma vez identificada uma incompatibilidade da estrutura tecnológica e humana com as condições de SegInfo estabelecidas pela corporação, ações de correção devem ser executadas. Infelizmente, na maioria das vezes são ações executadas sob grande tensão, como por exemplo na execução de Planos de Continuidade e de recuperação de desastres. È importante observar que um Plano de Continuidade de negócios é, na verdade, durante toda a sua existência uma ação preventiva, e apenas quando efetivamente executado reveste-se de uma ação corretiva.

UNIVER CIDADE

Conceitos Básicos de Segurança

- Risco
  - Probabilidade da exploração de alguma ameaça
- Impacto
  - Abrangência dos danos causados pela ocorrência de um incidente
- Incidente
  - Fato decorrente da exploração de uma vulnerabilidade por uma ameaça, gerando impactos nos processos de negócio da empresa

O risco está e sempre estará presente, e a meta deve ser controlar permanentemente o nível de risco num patamar estudado e estipulado de acordo com as diretrizes estratégicas do negócio. Traduz-se pela probabilidade em que uma ameaça explore efetivamente uma ou mais vulnerabilidades presentes, causando danos a um ou mais aspectos de SegInfo, comprometendo naturalmente o negócio.

O impacto é uma medida desse dano, ou seja, traduz-se pelos efeitos que esse incidente causou ou pode causar ao negócio. É subjetivo e depende de um profundo conhecimento do negócio. Veja esse exemplo: qual é a noção de impacto para seu filho adolescente numa eventual necessidade de se reformatar o disco rígido do seu PC por conta de uma infecção generalizada por vírus, spywares e outras pragas ? Certamente é muito menor do que a SUA noção de impacto desse mesmo incidente de segurança.

O incidente é decorrente da ação da ameaça explorando efetivamente uma vulnerabilidade. Estes incidentes geram impactos nos processos de negócio, e a extensão de sua gravidade pode ser avaliada e dimensionada em termos quantitativos e qualitativos, de acordo com os impactos provocados.

UNIVER CIDADE

Conceitos Básicos de Segurança

- Teoria do Perímetro
  - Segmentação inteligente dos ativos → permite a aplicação adequada de controles
- Barreiras de Segurança
  - Filósofo Shrek:
    - ✓ No campo de girassóis, a caminho de "salvar" a princesa Fiona
      - Por que não faz umas coisas de Ogro para assustá-lo? Estrangular, atacar o forte, moer ossos. Um kit completo de Ogro.
      - Eu sei. Eu poderia decapitar a vila toda, espetar as cabeças deles, pegar uma faca, abrir seus braços e beber seus fluidos. Gostou disso?
      - Não, na verdade não.
      - *Os Ogros são bem melhores do que as pessoas acham.*
      - Por exemplo?
      - Exemplo? Os Ogros são como cebolas.
      - Eles fedem?
      - Sim. Não!
      - Fazem vc chorar?
      - Não.
      - Se deixar sob o sol, ficam marrons.
      - Não! Camadas! As cebolas têm camadas. Os Ogros têm camadas! Entendeu? Ambos temos camadas.
      - Ahn! Ambos têm camadas. Não são todos que gostam de cebola. Bolo! Todos adoram bolo! Os bolos têm camadas.
      - Não me interessa o que as pessoas gostam. Os Ogros não são iguais a bolo.
      - Sabe do que mais todo mundo gosta? "Parfaits".
      - Não! Sua miniatura irritante e obtusa de burro de carga. Ogros são iguais a cebolas! Fim da história! Tchau.

Uma estratégia militar adaptada para o segmento de negócios, particularmente eficaz é e segmentação. Quando o problema é muito grande, segmentá-lo permite um tratamento mais adequado de acordo com nuances que são particulares a alguns grupos dentro do conjunto maior. Se segmentarmos o conjunto de ativos da empresa, podemos aplicar controles adequados à necessidade de cada grupo, sem que se exceda limites nem se fique aquém das necessidades de cada um. Um exemplo é a criação de grupos de usuários com necessidades distintas de acesso às informações armazenadas. Com isso, pode-se implementar o princípio do privilégio mínimo, evitando que usuários tenham mais acesso do que possam precisar, aumentando o nível de vulnerabilidades.

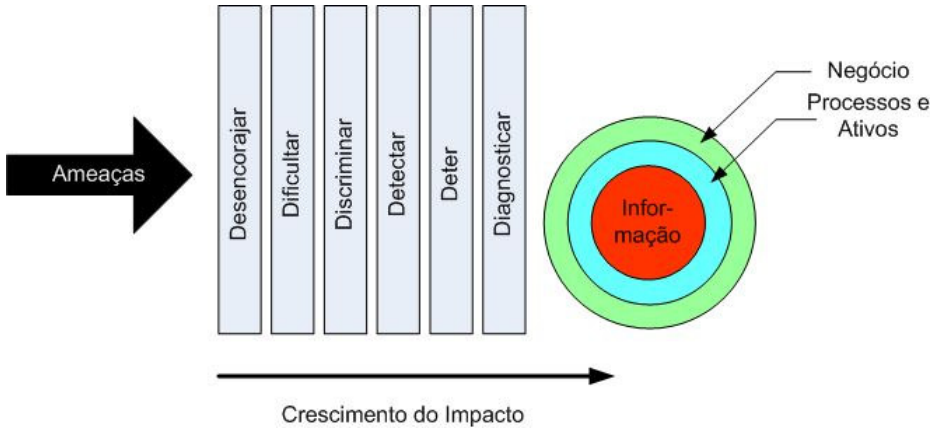
Outra estratégia militar adaptada para os negócios é a defesa em barreiras, ou seja, implementa-se camadas de segurança com objetivos e intensidades diferentes, visando desestimular ou dificultar o sucesso da ameaça desde o início de sua investida, e caso ele obtenha sucesso ao ultrapassar uma barreira, ele encontre outras com estratégias diferentes para evitar que ele obtenha sucesso. A maioria das companhias de seguro exigem que os vidros dos automóveis segurados sejam gravados com os números de chassis. Isso desestimula ladrões que desejem o carro para remarcação de chassis, falsificação de documentos e revenda, porque além do motos e do chassis ou vidros também terão que ser remarcados ou trocados. Normalmente o ladrão vai para o carro ao lado...

Para a implementação desta estratégia de segurança, deve-se segmentar o acesso à informação em perímetros físicos e lógicos, visando oferecer níveis diferenciados de resistência e proteção. Perímetros físicos são, por exemplo, área de recepção, circulação de pessoal, ambiente de produção e datacenter. Perímetros lógicos são o sistema de autenticação de visitantes, a Intranet, a Internet, Os sistemas críticos e os Bancos de Dados. Observe que em ambos os casos as necessidades de mecanismos de segurança são crescentes.

UNIVER CIDADE

Conceitos Básicos de Segurança

- Defesa em Camadas



Seg. Informação – Prof. Fred Sauer 45/117

A defesa em camadas prevê a a implementação de fases com níveis de resistência crescentes. O **Desencorajar** visa exclusivamente fazer com que as ameaças percam seu estímulo inicial para exploração de vulnerabilidades. Isso pode ser feito através de mecanismos físicos, tecnológicos ou humanos, implementando-se câmeras de vídeo (mesmo falsas ! Hoje em dia são muito comuns placas "sorria, você está sendo filmado" sem que exista uma câmera sequer), campanhas de divulgação da Política de Segurança, informação sobre os procedimentos de auditoria e Forense Computacional, etc. **Dificultar** é a segunda barreira. É complementar à anterior e visa a adoção efetiva de controles para dificultar o acesso indevido. Exemplos são roletas, detectores de presença com alarmes, senhas, certificados digitais, etc. **Discriminar** é a ação de identificar e gerir os acessos identificados na fase anterior, permitindo acessos apenas para quem precisa e no nível necessário. A **Detecção** visa identificar uma situação de risco, ou seja, a tentativa de alguém de burlar as ações da fase anterior. Exemplos dessas ações são os antivírus, sistemas IDS entre outros. **Deter** objetiva impedir que a ameaça atinja os ativos, caso as barreiras anteriores não tenham sido eficazes. Ações administrativas, punitivas, bloqueio de acessos físicos e lógicos são exemplos. **Diagnosticar** não é simplesmente o último passo dessa segmentação, por representar o elo de ligação com a primeira barreira, sendo portanto a mais importante para o aprimoramento das estratégias de defesa dos ativos. Um bom diagnóstico é representado por uma detalhada análise de riscos, que deverá corrigir rumos e atualizar estratégias de acordo com todo o dinamismo que cerca o ambiente de negócios.

UNIVERCIDADE

Conceitos Básicos de Segurança

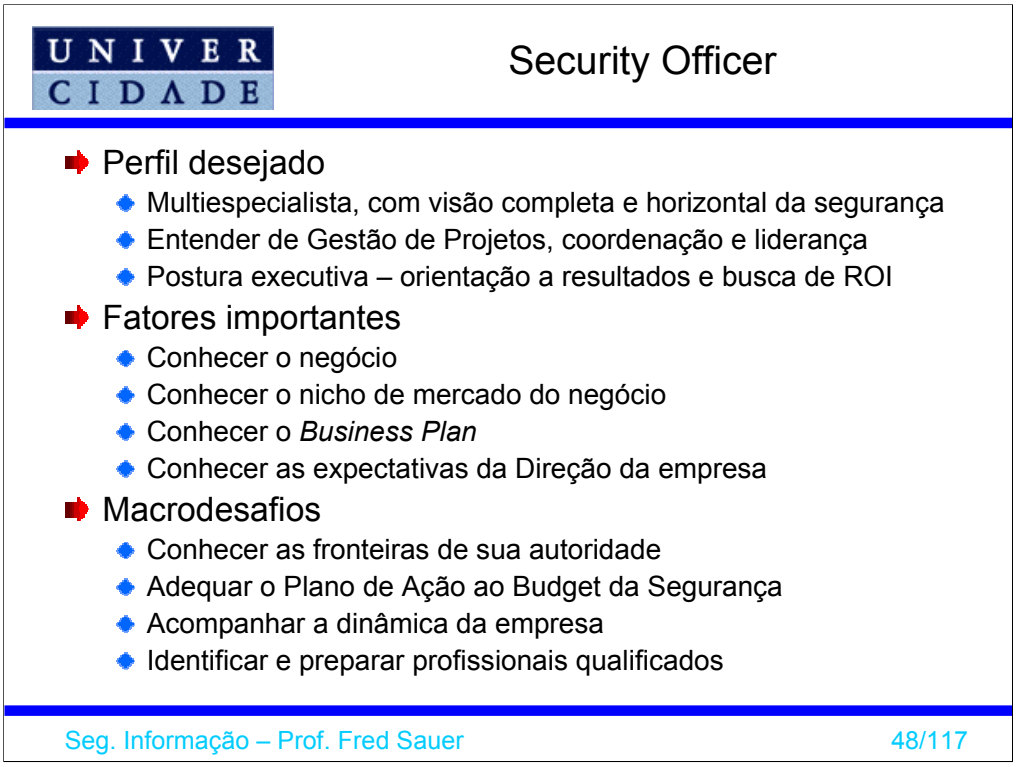
- Desencorajar
  - Câmera de vídeo visível, avisos de alarmes, treinamento
- Dificultar
  - Dispositivos de autenticação para acesso físico
- Discriminar
  - Identificar e gerir os acessos
- Detectar
  - Sinalização de situações de risco (ex.: antivírus e IDS)
- Deter
  - Ações administrativas, punitivas e bloqueios
- Diagnosticar
  - Análise de riscos, orientado ao negócio e direcionado para a primeira barreira

UNIVERCIDADE

Conceitos Básicos de Segurança

- Equação do Risco:
  - $R = \frac{V \times A \times I}{M}$

Todos os negócios, em função de suas peculiaridades, possuem um conjunto enorme de variáveis que influenciam direta e indiretamente o seu nível de risco. Estas variáveis devem ser agrupadas para permitir a avaliação desse nível de risco, em vulnerabilidades, ameaças, impactos e mecanismos de segurança. A equação do risco apresenta a relação entre estas variáveis. Fica fácil observar que, se quisermos reduzir ao máximo os **riscos** aos quais estamos submetidos, é necessário minimizar as **vulnerabilidades**, identificar as **ameaças** e implementar medidas eficazes para afastá-las, com o conhecimento dos **impactos** de um eventual incidente de segurança. Além disso, maximizar a eficácia dos **mecanismos** de segurança voltados para a redução desse nível de risco.



O *Security Officer* é um elemento atualmente presente na maioria das corporações, que tem alguns requisitos básicos para o seu sucesso. O primeiro deles é o perfil tecnológico essencialmente associado às características e necessidades do negócio, ajustando constantemente suas ações às premissas e definições estratégicas da empresa.

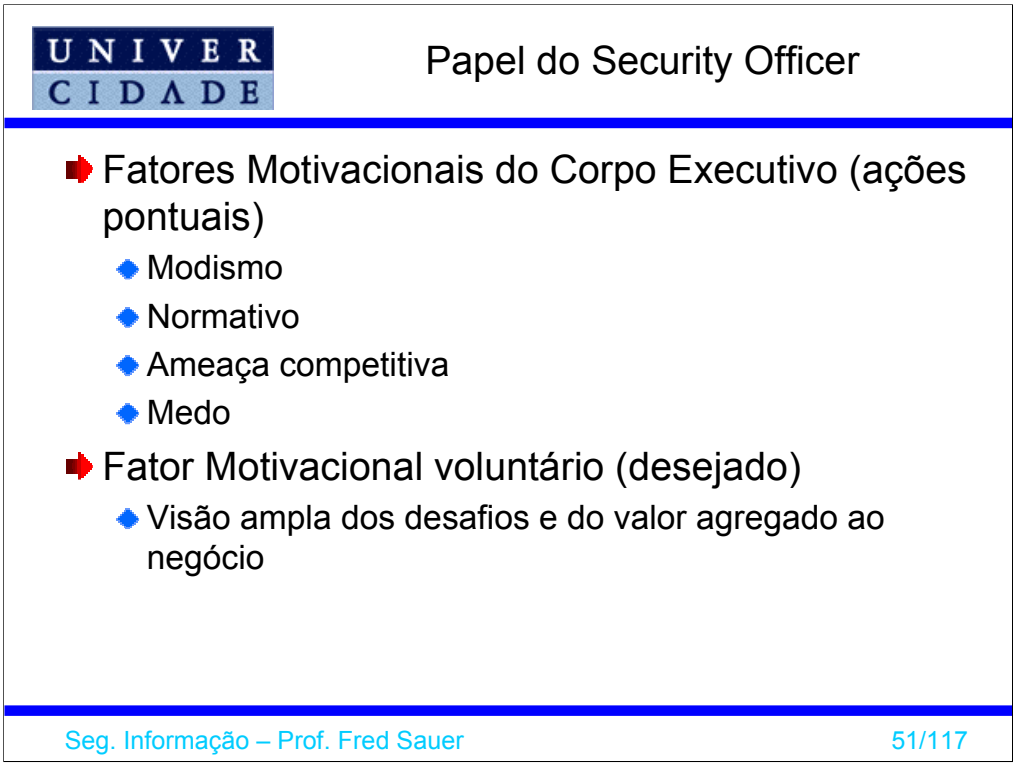
UNIVER CIDADE

Papel do Security Officer

É um papel desafiador, pois mesmo que tenha apoio e comprometimento do corpo executivo da empresa, e sempre enfrentará resistências que devem ser eliminadas através de negociação.

UNIVER CIDADE

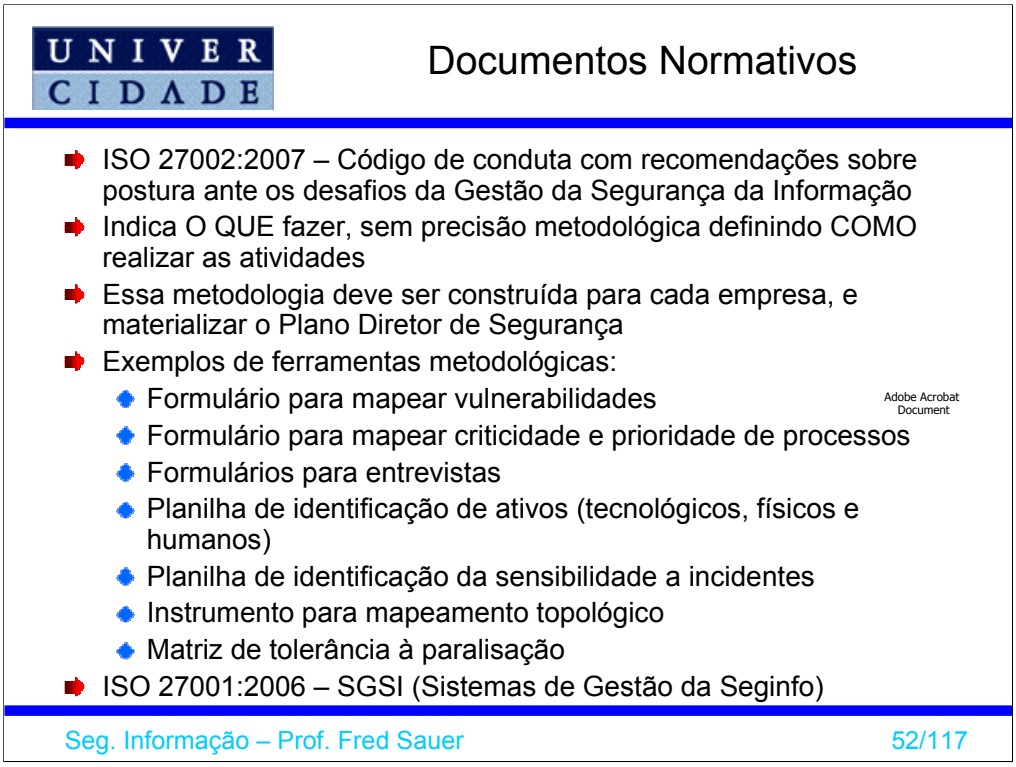
Perfil do Security Officer



Para essa negociação, é fundamental atingir pontos que sensibilizem as lideranças corporativas, convergindo para suas expectativas e principais interesses. Deve-se usar mensagens claras e objetivas. Comparar cenários vividos e almejados, com uma valorização clara dos benefícios. Usar o ROI, ferramenta executiva de tomada de decisões, sempre baseando-se em dados reais e que exponham claramente o valor agregado da iniciativa da SegInfo. Apenas se obterá êxito se o corpo executivo agir voluntariamente para o alinhamento com as ações de SegInfo.

Os principais motivos que podem conduzir o corpo executivo a agir voluntariamente são o **modismo** (opinião pública), **Normativo** (regras e regulamentos externos), **Ameaça da concorrência** (como espionagem industrial em projetos estratégicos), **Medo** (motivado pela percepção opaca e parcial dos riscos envolvidos), **Desastre** (fator reativo devido a fatos já consumados) e, principalmente, o perfeito **entendimento** dos benefícios de uma solução corporativa de SegInfo.

Um instrumento particularmente poderoso é o **teste de invasão**, que permite a avaliação das vulnerabilidades existentes e normalmente tem resultados preocupantes, conferindo ao *Security Officer* maior poder de persuasão e convencimento.



Muitos são os desafios da SegInfo, que tendem a crescer ainda mais com o surgimento de novas tecnologias, modelos de negócio e inovações no relacionamento comercial, cada vez mais eletrônico. Neste cenário, nada melhor do que a disponibilidade de um *framework* básico que possa ser usado como linha básica, adaptando os procedimentos às peculiaridades de cada empresa. A comunidade britânica criou então a norma BS7799, que rapidamente passou a ser adotada por várias outras comunidades mundo afora. A ISO analisou a norma e adotou-a, levando a identificação ISO 17799:2000 (primeira versão). A ABNT, braço da ISO no Brasil, disponibilizou então a versão NBR ISO/IEC 17799-1, com pequenos ajustes à realidade brasileira. O objetivo desta norma é criar uma "base comum" para a criação de normas internas nas empresas, agregando valor ao processo mercadológico através da redução dos riscos em todos os elementos da cadeia produtiva, provendo confiança nos relacionamentos entre as organizações. Apenas a parte 1 da norma (Código de Conduta) está disponível. A parte 2, referente aos requisitos para sistemas de gerenciamento da Segurança da Informação, foi publicada em Genebra em 15 de outubro de 2005, e estima-se para o primeiro trimestre de 2006 a prontificação de uma versão brasileira pela ABNT. Espera-se que, assim como aconteceu com a ISO 9000, a certificação da empresa em segurança da informação também se torne um requisito de qualidade entre os parceiros da cadeia produtiva.

Como qualquer norma, diz apenas O QUE fazer, sem precisão metodológica de COMO fazer. É um grande manual, que deve ser usado na construção do Plano Diretor de segurança de cada empresa.

Há várias ferramentas metodológicas que podem ser usadas para elaborar análises e mapear as necessidades de SegInfo para cada empresa. No *slide* estão citadas algumas delas, porém não apenas uma única metodologia recomendada.

UNIVERCIDADE

Status SegInfo

- **Brasil (18)**: Serasa, *Banco Matone*, *Samarco*, Módulo Security, Unisys, *PRODESP*, SERPRO, Telefônica, Atos Origin, CIP, FUCAPI, Promon, Tivit, T-Systems, Axur, Zamprogna Importação. (http://www.iso27001certificates.com/Taxonomy/CertificateSearch.htm)
- **ISO 27000** - Vocabulário de Gestão da Segurança da Informação (sem data de publicação).
- **ISO 27001** - Esta norma foi publicada em Outubro de 2005 (revisada em 2006) e substituiu a norma BS 7799-2 para certificação de Sistemas de Gestão de Segurança da Informação.
- **ISO 27002** – Em 01/07/2007 esta norma substituiu a ISO 17799:2005 (Código de Boas Práticas).
- **ISO 27003** - Esta norma abordará a gestão de risco, contendo recomendações para a definição e implementação de um sistema de gestão de segurança da informação. Deverá ser publicada em 2008 ou 2009. Seu título provisório é: "*Information technology - Security techniques. Information security management system implementation guidance*".
- **ISO 27004** - Esta norma descreverá métricas para avaliação de sistemas de gestão de segurança da informação.
- **ISO 27005** - Esta norma será constituída por indicações para implementação, monitoramento e melhoria contínua do Sistema de Controles de Risco. O seu conteúdo deverá ser idêntico ao da norma BS 7799-3:2005 – "*Information Security Management Systems - Guidelines for Information Security Risk Management.*
- **ISO 27006** - Esta norma disciplinará os órgãos de certificação e auditoria. Este documento terá o título de "*Information technology - Security techniques. Requirements for bodies providing audit and certification of information security management systems*".

UNIVER CIDADE

Postura do Security Officer

- Empenhar-se no macro-desafio da solução de segurança: SEGMENTAÇÃO e CONTROLE para condução/manutenção do risco aos patamares aceitáveis
- Atitude PDCA (ISO 9001)

Security Officer é o elemento responsável por coordenar as ações de implementação da SegInfo. É tarefa das mais desafiadoras e demanda não apenas responsabilidades, mas principalmente ferramentas e apoio executivo. O maior desafio deste elemento traduz-se na palavra CONTROLE. Com isso, pode-se administrar vulnerabilidades e reduzir riscos. Pode-se, por exemplo, decidir autorizar ou bloquear acessos a áreas sensíveis; registrar tentativas de acesso indevidas, reagindo para impedir sabotagem, fraude ou roubo de informações; definir estratégias para manipulação de dispositivos de armazenamento, e-mail, etc. Nunca se deve confundir CONTROLE – atividade desejada – com BLOQUEIO ou PROIBIÇÃO, que são ineficazes por natureza. Outra atividade importante para os desafios do Security Officer é a SEGMENTAÇÃO, por permitir que se implemente níveis de segurança diferentes para necessidades diferentes.

A norma BS7799 parte 2 sugere a adoção da postura PDCA (Plan – Do – Check – Act), cujo modelo é citado na ISO 9001, e tem perfeita adequabilidade aos estudos conceituais de segurança vistos até agora. Planejar – Implementar – Analisar – Monitorar. Essas 4 fases são aplicáveis na organização de todas as atividades que fazem parte da solução de segurança, bem como todas as atividades decorrentes, ou seja, orientam as ações tanto do nível executivo (estratégico) como dos níveis tático e operacional. É natural que a percepção dos resultados é adequado para cada nível, sendo no nível executivo observado o comportamento do negócio em si, no nível tático mudanças nos indicadores dos sistemas de gestão e no nível operacional mudanças físicas, tecnológicas e humanas.

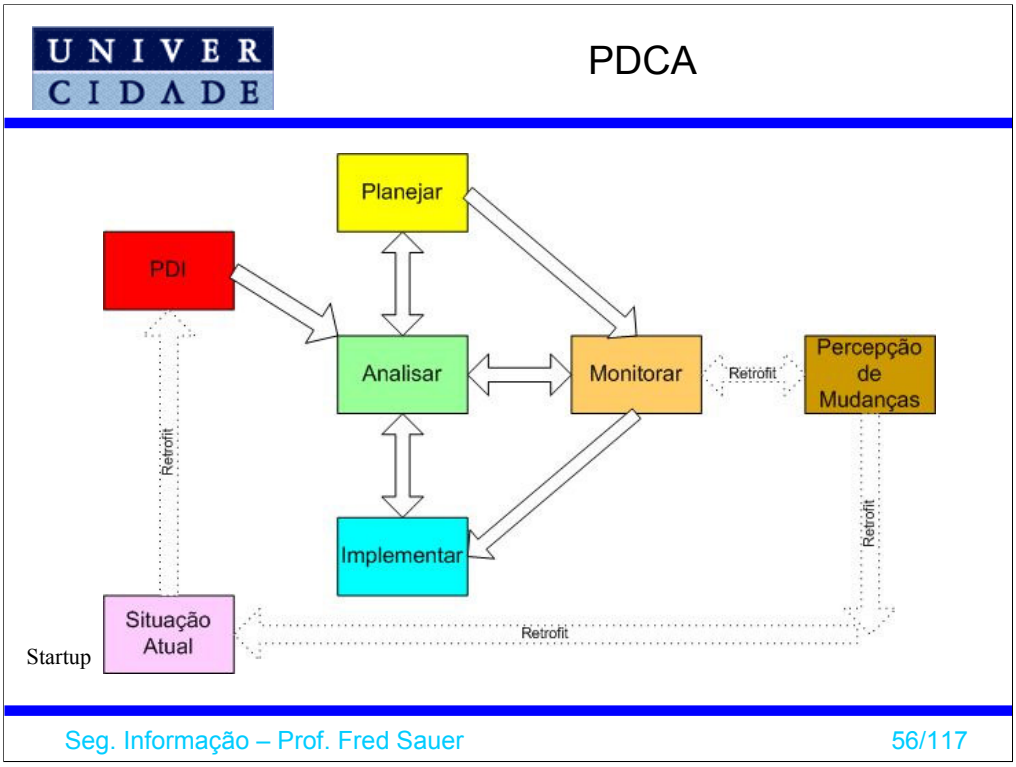
Podemos dizer que é necessário **planejar** as ações executivas (Plano Diretor de Segurança – Nível estratégico) para realizar investimentos adequados e organizar o *Security Office*. Da mesma forma, é necessário **analisar** os fatores de risco que orientarão as ações de segurança decorrentes. Pode-se então **implementar** os controles físicos, tecnológicos e humanos, e a seguir **monitorar** os resultados e os novos elementos que porventura surjam (como vulnerabilidades e ameaças), visando a retro-alimentação do sistema.

Na fase de **Planejamento** pretende-se definir arquiteturas, ações, atividades, alternativas de continuidade e critérios, abrangendo todo o ciclo de vida da informação. Terá como resultados práticos o Plano Diretor de Segurança, o Plano de Continuidade dos Negócios e a Política de Segurança da Informação.

A fase de **Análise** compreende atividades para geração de um diagnóstico de segurança, mapeando particularidades físicas, tecnológicas e humanas como um todo ou através de perímetros, com a identificação de vulnerabilidades, ameaças, riscos e impactos que podem se refletir no negócio. Nesta fase busca-se construir a análise de riscos e pode-se usar como ferramenta de descoberta de vulnerabilidades o teste de invasão.

A fase de **Implementar** compreende as atividades que efetivamente aplicam mecanismos de controle nos ativos físicos, tecnológicos e humanos, buscando reduzir ao máximo suas vulnerabilidades, buscando com isso aumentar o nível de segurança do negócio. Nesta fase se materializam as ações organizadas pelo planejamento e particularizadas através do diagnóstico (análise). São implementados "Controles de Segurança" e realizados "Treinamentos e Sensibilização em Segurança".

A fase de **Monitorar** empreende ações para gerir o nível de segurança, através de indicadores e índices capturados no sistema, permitindo uma percepção dinâmica do grau de risco vivido pelo negócio. Realiza a realimentação do sistema continuamente, implementando um processo de gestão dinâmica. Compõe essa fase as equipes de resposta de incidentes e a administração e monitoração de Segurança.



Essa figura ilustra a interação entre as fases, destacando a importância da fase de monitoramento, que interage com todas as outras permitindo a Gestão Dinâmica através da correção de rumos de acordo com a percepção do ambiente existente.

Na cronologia dos eventos, antes de tudo é importante **analisar**, e em função dessa análise gerar (**planejar**) a primeira versão do Plano Diretor de Segurança. **Implementam-se** os comitês de segurança, atribui-se responsabilidades, inicia-se um programa de divulgação, treinamento e conscientização. Inicia-se a tarefa de **monitoramento** desde então, realimentando a **análise** de riscos. Com essa realimentação, novamente se **planejam** ações, **implementam-se** controles e **monitoram-se** resultados, para que se possa realizar novas análises e assim por diante.

Plano Diretor de Segurança

- Deve ser dinâmico e flexível
- Apontará o caminho e os passos para suprir as necessidades de segurança do negócio para operação sob risco controlado
- Modelagem de um PDS
  - Profundo conhecimento do negócio (*Business Plan*)
  - Levantamento de informações do negócio (são identificadas ameaças, vulnerabilidades, riscos e impactos potenciais)
  - Mapear relevância dos processos críticos
  - Estudar Impactos (CIDAL)
  - Estudo de Prioridades (GUT)
  - Estudo de Perímetros
  - Estudo de Atividades

O Planejamento é fator crítico de sucesso para a SegInfo, e o Plano Diretor de Segurança (PDS) é o instrumento para este fim. Deve ser **dinâmico e flexível**, apontando o **caminho e os passos** (atividades) para a **implementação da solução** e atender às necessidades de segurança do negócio, de forma a operar sob **risco controlado**. É peculiar a cada empresa, e por isso não há como usar um outro modelo, por mais sucesso que tenha se obtido através dele.

O início da modelagem de um PDS está relacionado com o levantamento de informações do negócio, em busca das vulnerabilidades, ameaças potenciais, impactos e conseqüentemente, riscos. Para isso, é fundamental conhecer profundamente as regras do negócio, bem como as demandas decorrentes do *business plan*. Nesta fase inicial mapeia-se o relacionamento entre os processos de negócio e a infra-estrutura física, tecnológica e humana da empresa, através das aplicações que manipulam as informações. É um processo de auto-conhecimento. Com esse mapeamento, pode-se iniciar o processo de construção do PDS, composto de 6 etapas citadas a seguir.

UNIVER CIDADE

Metodologia para o PDS

- Identificação dos Processos do Negócio
  - Resultados esperados:
    - ✓ Mapeamento dos Processos Críticos para a operação da empresa
    - ✓ Identificação dos gestores-chave dos processos mapeados
    - ✓ Início da integração e comprometimento dos gestores-chave
    - ✓ Início do entendimento do funcionamento do negócio
- Mapeamento da Relevância
  - Resultados esperados:
    - ✓ Mapeamento da relevância dos processos de negócio críticos
    - ✓ Envolvimento dos gestores com visão holística do negócio
    - ✓ Percepção dos fatores importantes considerados pelos gestores envolvidos

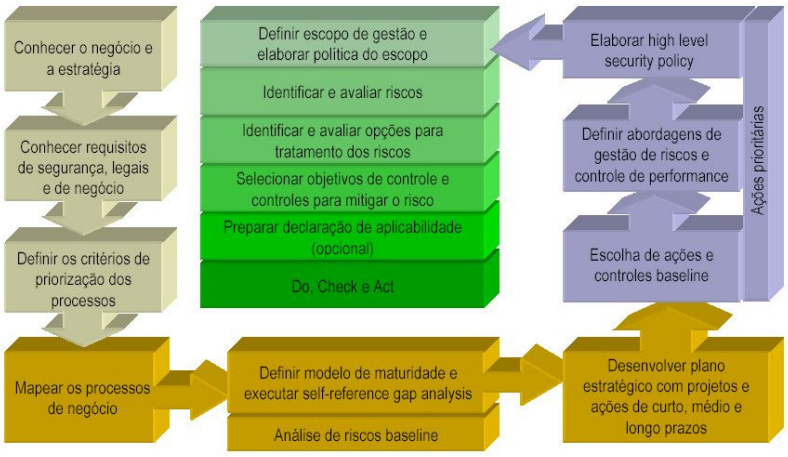
A identificação dos processos de negócio críticos que serão o alvo das atividades de SegInfo podem ser conhecidos através de entrevistas e *brainstorm* com os principais gestores com representatividade na empresa. São fundamentais a identificação dos processos mais sensíveis e as necessidades físicas, tecnológicas e humanas para que cada um deles possa suportar o negócio como um todo. Estes são os ativos a serem protegidos.Nessa identificação, é importante utilizar unidades de medida compatíveis com os processos em questão e suas variáveis, de forma a permitir um diferenciamento em termos de sensibilidade. Por exemplo, para um processo de negócio PN1, as variáveis receita e margem são medidas em $ e %, respectivamente. Este mesmo PN pode ter sua componente estratégica avaliada através de um peso, para poder compará-lo adequadamente com os demais. Os resultados esperados estão citados no slide.

No Mapeamento da Relevância, já se conhece os PN e suas variáveis, e nível de sensibilidade para a continuidade do negócio. Agora deve-se mapear a relevância de cada um deles, de forma que se possa priorizar objetivamente as atividades que comporão a solução, dedicando mais investimento onde for mais sensível. Nesta fase é importante o envolvimento de gestores com a visão corporativa necessária para orientar essa priorização, com imparcialidade e visão global do negócio. O próximo slide mostra um instrumento de mapeamento de relevância, a ser aplicado na avaliação dos PN quanto à sua criticidade.

UNIVER CIDADE

Metodologia para o PDS

Visão funcional
Planejamento Estratégico



Fonte:www.semola.com.br

UNIVERCIDADE

Neste Curso

- **Atividades e suas Finalidades**
  - **Mapeamento dos PN** → compreensão do negócio
  - **Elenco de ativos, de acordo com a sua natureza** → Identificar os componentes do problema do risco
  - **Correlação entre Ativos x Informação x ciclo de vida** → identificar as relações dos componentes do problema com a informação
  - **Identificação de algumas ameaças e vulnerabilidades visíveis**, de acordo com as entrevistas realizadas com os gestores dos PN → Proposição futura da 1ª versão da PolSeg
  - **CIDAL** – aferição do nível de sensibilidade à incidentes de segurança, de acordo com cada aspecto (confidencialidade, integridade, disponibilidade, autenticidade e legalidade), obtendo uma avaliação média da sensibilidade do PN com objetivo de priorização
  - **GUT** – Prioridade global entre os PN, através da agregação da componente "tolerância à paralisação" e a "tendência de agravamento", no decorrer do tempo.
  - **BIA** – Evidenciar necessidades precisas de contingenciamento, de acordo com a tolerância temporal e a prioridade entre os processos
  - **PLCONT** – Contingenciar PN através de seus ativos, de acordo com o BIA
  - **PolSeg** – Propor controles objetivos para o cenário compreendido, na forma de diretrizes, normas e procedimentos
  - **Análise de Riscos** – Avaliação do Nível de Risco para realimentar o processo

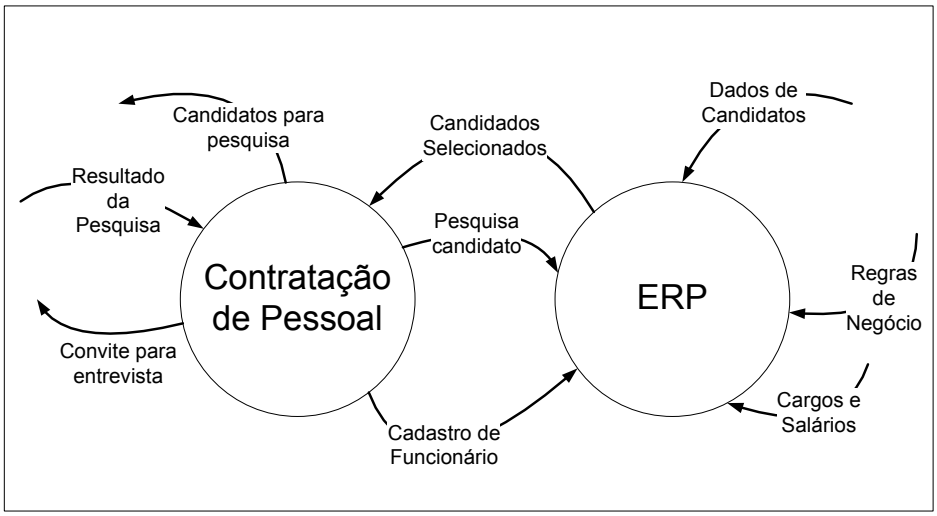
UNIVERCIDADE

Estudo de Caso – Parte 1

- Identificação dos PN
- Mapeamento de Entradas e Saídas
- Identificação de Ativos e correlação com o ciclo de vida da Informação
- Identificação das variáveis que afetam o negócio

UNIVERCIDADE

Mapeamento



UNIVERCIDADE

Ativos

	PN A	PN B
Físicos	Salas, Mobiliário, infra-estrutura de dados e voz, cofre	Salas, Mobiliário, infra-estrutura de dados e voz
Tecnológicos	XXX	ERP (sistema)
Físico-tecnológicos	Computadores, equipamentos de conectividade locais	Computadores, equipamentos de conectividade locais
Humanos	Gestor	Gestor, técnicos

UNIVER CIDADE

Ciclo de Vida da Informação – PN A

Ativo		Fase Ciclo	Info
PN A	Salas, mobiliário	Armazenamento	Todas (em forma visível ou audível)
	Cofre	Armazenamento	Resultado da Pesquisa (impressa)
	Infra-estrutura de dados, equipamentos de conectividade locais	Transporte	Todas, exceto o convite para entrevista
	Infra-estrutura de voz	Transporte	Convite para entrevista
	Computadores	Armazenamento	Todas, exceto o convite para entrevista
	Gestor	Manipulação	Todas
	Gestor	Descarte	Qualquer Info impressa referente ao candidato

UNIVERCIDADE

Algumas Variáveis Impactantes

Ameaça		Vulnerabilidade
PNA	Candidato com dados expostos (processo judicial)	Funcionário do setor (Tratamento inadequado da informação sigilosa)
	Qualquer	Gestor de PN sem cultura de segurança
PNB	Pane elétrica	Empresa fornecedora de energia de baixa qualidade
	Sabotador	Acesso fácil de estranhos
	Técnico mal-intencionado	Customização do sistema
	Qualquer	Gestor de PN sem cultura de Segurança

UNIVERCIDADE

Observações desta Fase

- Os resultados são imprecisos e, muitas vezes, contraditórios
- É importante discutir com os Gestores dos PN buscando a visão holística
- O foco deve sempre ser a **informação**

UNIVERCIDADE

Identificação de PN críticos

	Clientes Atendidos	Receita	Margem	Fator Estratégico	Conformidade Legal
PN 1	N				
PN 2		$			
PN 3			%	Peso	$ multa

A coluna da direita busca dar um caráter mais elucidativo às decisões, e deve ser particularizado à corporação em questão. Essa coluna é que possui as respostas a serem buscadas, ou seja, apenas a parte qualitativa da análise. A coluna da esquerda, o resultado quantitativo buscado, deve ser avaliado de forma holística para permitir a priorização das atividades.

UNIVER CIDADE

PDS – Estudo dos Impactos (CIDAL)

- Estudo CIDAL
  - Resultados esperados
    - ✓ Classificação da sensibilidade CIDAL para cada processo de negócio
    - ✓ Envolvimento dos gestores com visão isolada dos processos específicos
    - ✓ Percepção dos fatores importantes considerados pelos gestores envolvidos

Uma vez identificados os PN críticos, já se pode evoluir para um maior detalhamento da sensibilidade de cada um deles a incidentes de segurança, especificamente relacionados com os aspectos de segurança já discutidos – CIDAL – Confidencialidade, Integridade, Disponibilidade, Autenticação e Legalidade. Os mesmos critérios quantitativos de avaliação da fase anterior podem ser utilizados, porém agora avaliando cada PN isoladamente. O slide seguinte apresenta uma matriz para elaboração dessa avaliação. Os resultados esperados desta etapa estão descritos no slide.

UNIVERCIDADE

PDS – Estudo dos Impactos (CIDAL)

Processo de Negócio 1		Conceitos			Aspectos	
Escala		CONFIDENCIALIDADE	INTEGRIDADE	DISPONIBILIDADE	AUTENTICIDADE	LEGALIDADE
1	não considerável					
2	relevante					
3	importante					
4	crítico					
5	vital					

Tabela de escalas para classificação de sensibilidade dos processos de negócio.

UNIVERCIDADE

PDS – Estudo de Prioridades (GUT)

- Estudo GUT
  - Matriz de GUT (Gravidade, Urgência e Tendência)
  - Critérios:
    - ✓ Gravidade – qual é o nível de severidade em uma eventual quebra de segurança ?
    - ✓ Urgência – deve levar em conta o tempo de duração dos impactos
    - ✓ Tendência – qual é a tendência dos riscos se nenhuma atividade preventiva ou corretiva for aplicada ?
  - Resultados esperados:
    - ✓ Mapeamento da prioridade global de cada processo de negócio
    - ✓ Percepção das características de cada processo em função da análise GUT

Com a ajuda do principal gestor de cada PN que teve sua classificação avaliada como crítica, pode-se estudar e pontuar a prioridade, através da conhecida matriz de GUT: Gravidade, Urgência e Tendência. A prioridade final é composta pela análise e pelo produto das três dimensões do GUT.

Gravidade – seria muito grave para o PN avaliado se algum incidente de segurança comprometesse um ou mais aspectos CIDAL ? Esta pergunta deve ser respondida considerando a severidade dos impactos. Por exemplo: O que ocorreria com o PN de Aprovação de Crédito de uma financeira se a base de dados de clientes fosse corrompida, comprometendo sua integridade ?

Urgência – Havendo um incidente de segurança, independentemente de qual aspecto CIDAL tenha sido comprometido, qual seria a urgência da solução para os efeitos desse incidente suportável para o negócio ? Cabe ressaltar a importância da consideração do tempo de duração dos impactos associados ao PN analisado. No exemplo anterior, se a base de dados de clientes permanecesse corrompida por 2 dias consecutivos ?

Tendência – Considerando-se os planos de curto, médio e longo prazo de evolução do PN analisado, qual seria a tendência dos riscos se nenhuma atividade preventiva ou corretiva fosse aplicada ? essa linha de análise considera a oscilação da importância dos impactos. Complemente-se a análise do exemplo anterior com o seguinte questionamento: se a mesma base de dados fosse corrompida hoje, daqui a dois meses e daqui a dois anos, qual seriam as conseqüências em relação às tendências desse PN ?

O próximo slide apresenta uma tabela para estas avaliações.

UNIVERCIDADE

Matriz de GUT - Critérios

Gravidade		Urgência		Tendência	
1	sem gravidade	1	sem pressa	1	não agravará
2	baixa gravidade	2	tolerante à espera	2	agravará a longo prazo
3	média gravidade	3	o mais cedo possível	3	agravará a médio prazo
4	alta gravidade	4	com urgência	4	agravará a curto prazo
5	gravidade muito alta	5	imediatamente	5	agravará imediatamente

Devem ser atribuídos pontos para cada questionamento, mais uma vez com o uso da expressão qualitativa da situação. estes valores devem ser multiplicados para obtenção de um resultado final que oscilará entre 1 e 125. Com os resultados obtidos, conclui-se o mapeamento de prioridades para cada um dos PN e obtém-se a percepção das características da cada PN em função das dimensões do GUT.

UNIVER CIDADE

Estudo de Caso – Parte 2

- Avaliação preliminar da criticidade dos PN
- Avaliação CIDAL dos PN
- GUT dos PN

UNIVERCIDADE

Criticidade Relativa

Processo de Negócio	Fator Estratégico	Tolerância Temporal	Volume Mensal Movimentado (Receita)	Índice
Captação	5	4	2	**3,7**
Faturamento	5	5	5	**5**

UNIVERCIDADE

Parâmetros para Avaliação

Índice	Nível	Enquadramento
1	**Não Considerável**	A ocorrência de um incidente de segurança (IS) neste PN é absorvida integralmente através de um Plano de Continuidade de baixo custo sem prejuízo algum à atividade produtiva
2	**Relevante**	A ocorrência de um IS no PN em análise demanda ações reativas programadas perceptíveis em outros PN, podendo causar impactos de baixa monta, como pequenos atrasos ou prejuízos financeiros absorvíveis, porém indesejados
3	**Importante**	Um IS no PN em avaliação provoca a redução imediata de sua operacionalidade normal, causando prejuízos diários. Demanda ações reativas emergenciais para que a extensão de seus impactos não afetem outros PN da empresa e metas da empresa
4	**Crítico**	Os impactos de um IS podem ser percebidos em vários PN associados, 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.
5	**Vital**	A ocorrência de um IS deste tipo no PN em análise pode atingir toda a empresa e seus parceiros, causando impactos irreversíveis e demandando ações emergenciais que envolvem desde o setor estratégico até o operacional. Se persistente, pode provocar a falência da empresa

UNIVERCIDADE

CIDAL Captação (PN A)

	C	I	D	A	L
Não Considerável			X		
Relevante		X		X	
Importante	X				X
Crítico					
Vital					

Média: 2,2 (Relevante)

No PN A, a **CONFIDENCIALIDADE** e a **LEGALIDADE** são **IMPORTANTES**, considerando-se como evento mais sensível o comprometimento do relatório de investigação de um candidato. Tal evento poderia gerar processos judiciais desagradáveis para a empresa. A **INTEGRIDADE** e a **AUTENTICIDADE** são avaliadas como **RELEVANTES**, tomando como parâmetro a possibilidade da obtenção de relatórios forjados abonando a contratação de funcionários inidôneos. A **DISPONIBILIDADE** é **NÃO CONSIDERÁVEL**, já que o processo tem grande tolerância temporal, permitindo a construção de soluções alternativas.

UNIVER CIDADE

CIDAL Faturamento (PN B)

	C	I	D	A	L
Não Considerável					
Relevante					X
Importante					
Crítico	X			X	
Vital		X	X		

Média: 4 (Crítico)

No PN B, a **CONFIDENCIALIDADE** e **AUTENTICIDADE**, são CRÍTICAS, uma vez que o sistema armazena todas as informações estratégicas da empresa, inclusive os dados sigilosos dos funcionários citados no PN A. Um incidente como o vazamento do arquivo de informações sigilosas referentes aos funcionários pode gerar reações em toda a empresa, com grandes e desagradáveis efeitos. A **INTEGRIDADE** e a **DISPONIBILIDADE** são VITAIS, já que se trata de um ERP, onde toda a informação necessária para operação da empresa está armazenada. Dados incorretos ou indisponíveis podem conduzir à não-concretização de negócios ou decisões incorretas, que persistentes podem comprometer a saúde financeira da empresa. A **LEGALIDADE** é RELEVANTE, imaginando-se a necessidade de observar aspectos legais para a implementação das regras de negócio sem ferir a legislação vigente e aspectos éticos que possam trazer prejuízos à empresa.

UNIVER CIDADE

GUT – Tabela de significados

	Gravidade (CIDAL)	Urgência	Tendência
1	Entre 1 - 2,3	Tolerância acima 120h	Não há menção no PN*
2	Entre 2,4 - 3,7	Tolerância entre 24 e 120h	Possibilidade de agrava-mento prevista no PN
3	Entre 3,7 - 5	Tolerância inferior 24h	Previsão de incremento previsto no PN

*PN – Aqui, significa Plano de Negócios.

UNIVERCIDADE

GUT

	Gravidade	Urgência	Tendência	Total
PNA	**1**	**1**	**1**	**1**
PNB	**3**	**3**	**1**	**9**

Prioridade entre os processos: PNB, mais prioritário que o PNA, o que significa que o PNB é mais sensível, com maior nível de risco que o PNA.

UNIVER CIDADE

Conclusões desta Fase

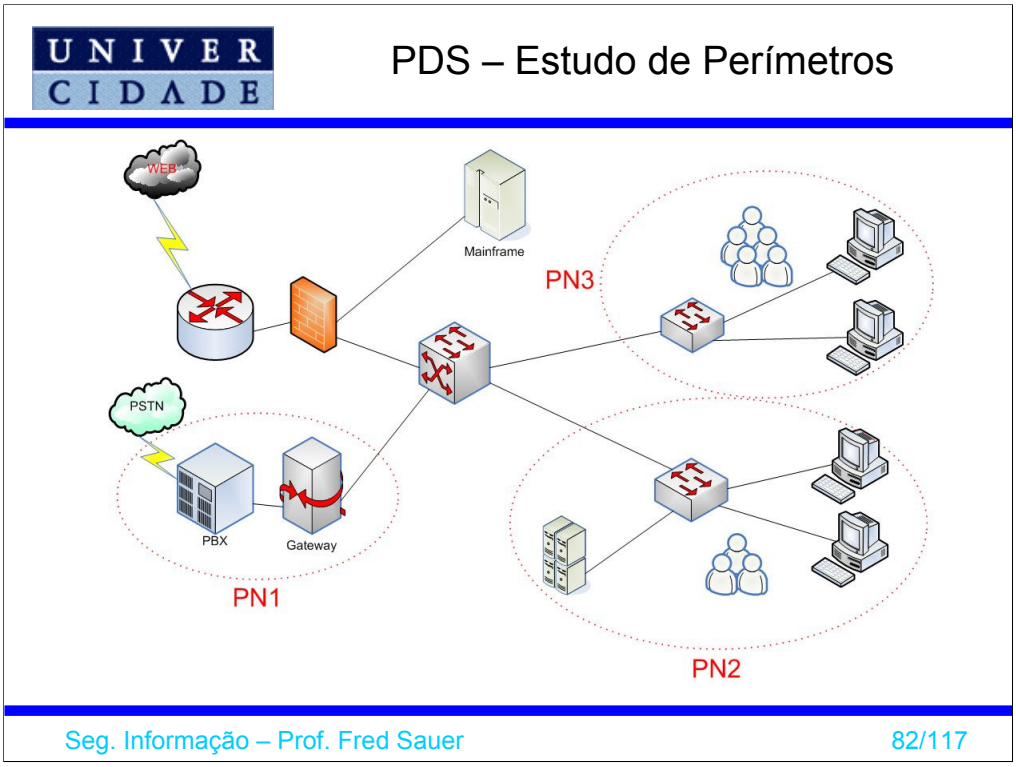
- O nível de entendimento é maior pela necessidade de avaliações comparativas
- Os modelos permitem verificar se as decisões anteriores foram adequadas, facilitando a revisão do modelo de negócio focado na informação

UNIVER CIDADE

PDS – Estudo de Perímetros

- Análise dos ativos que sustentam cada um dos processos de negócio
  - Infra-estrutura, tecnologia, aplicações, informações e pessoas
  - Devem ser usados plantas baixas, mapas topológicos, inventário de equipamentos, sistemas e aplicações
- Resultado esperado:
  - Mapeamento dos ativos
  - Mapeamento da relação entre ativos e processos de negócio

O PDS objetiva a montagem de um mapa de relacionamentos e dependências entre PN, aplicações e Infra-estrutura física, tecnológica e humana. Após a conclusão das etapas anteriores, inicia-se o estudo dos ativos que sustentam cada um dos PN, com a identificação dos alvos de infra-estrutura que tem ralação direta e indireta com cada um dos PN. Conhecendo-se os PN, identificam-se os ativos que sustentam e suportam os PN. Estes ativos, por sua vez, possuem vulnerabilidades que deverão ser minimizadas ao máximo. Nessa fase, diferentemente das anteriores, as fontes de consulta são os gestores da esfera técnico-tática, uma vez que serão necessárias informações topológicas, físicas e tecnológicas, obtidas através de plantas baixas, mapas topológicos, inventários de equipamentos, sistemas e aplicações. de posse destas informações, agrupam-se os ativos de acordo com suas similaridades em relação aos PN, definindo-se com isso vários perímetros.



Essa figura ilustra a definição de perímetros onde ativos são localizados dentro das fronteiras de determinados Processos de Negócio. Cabe ressaltar que nesses perímetros estão alocados ativos físicos, tecnológicos e humanos. Os ativos que não estão alocados especificamente a um ou outro PN suportam todos os PN ilustrados.

PDS – Estudo das Atividades

- Planejamento de ações para cada ambiente definido (perímetro), sempre de acordo com as diretrizes de segurança da empresa
- Ações de análise e interpretação das informações coletadas, cruzando-as com os planos de negócio, recursos disponíveis, níveis de segurança atual e recomendado
- Esta etapa inicia o processo de materialização do PDS, indicando atividades/projetos necessários de acordo com a prioridade aferida
- Todo trabalho deve ser coordenado pelo Security Officer , que tem a atribuição de liderar o Comitê Corporativo de Segurança, que por sua vez deve contar com Comitês (representantes) Departamentais

Nesta etapa, com os resultados das etapas anteriores pode-se planejar as ações específicas para ambientes e perímetros distintos, e isolados, porém que serão coordenadas e principalmente deverão estar em conformidade com as diretrizes de segurança corporativa estabelecida. que foram propostas pelo modelo de Gestão Corporativa de Segurança da Informação. O Estudo das Atividades inicia o processo de elaboração do PDS, indicando as atividades e projetos necessários distribuídos ao longo do tempo e de acordo com as prioridades extraídas da percepção de relevância dos Processos de Negócio.

Paralelamente com as atividades anteriores, é fator crítico de sucesso a organização da estrutura de *Security Office* (Comitê Corporativo de Segurança), cuja primeira responsabilidade é definir responsabilidades de planejamento, execução, monitoramento, inclusão na estrutura organizacional (com a garantia de acesso direto à alta administração). Divulgação interna com a participação efetiva de elementos de todas as áreas.

Os Comitês Departamentais tem grande importância, porque agem numa esfera de abrangência menor, porém com as mesmas diretrizes que toda a empresa, possibilitando uma precisa medição de resultados, percepção de novas necessidades e novas situações de risco. É o responsável pela ação local orientado por uma visão global.

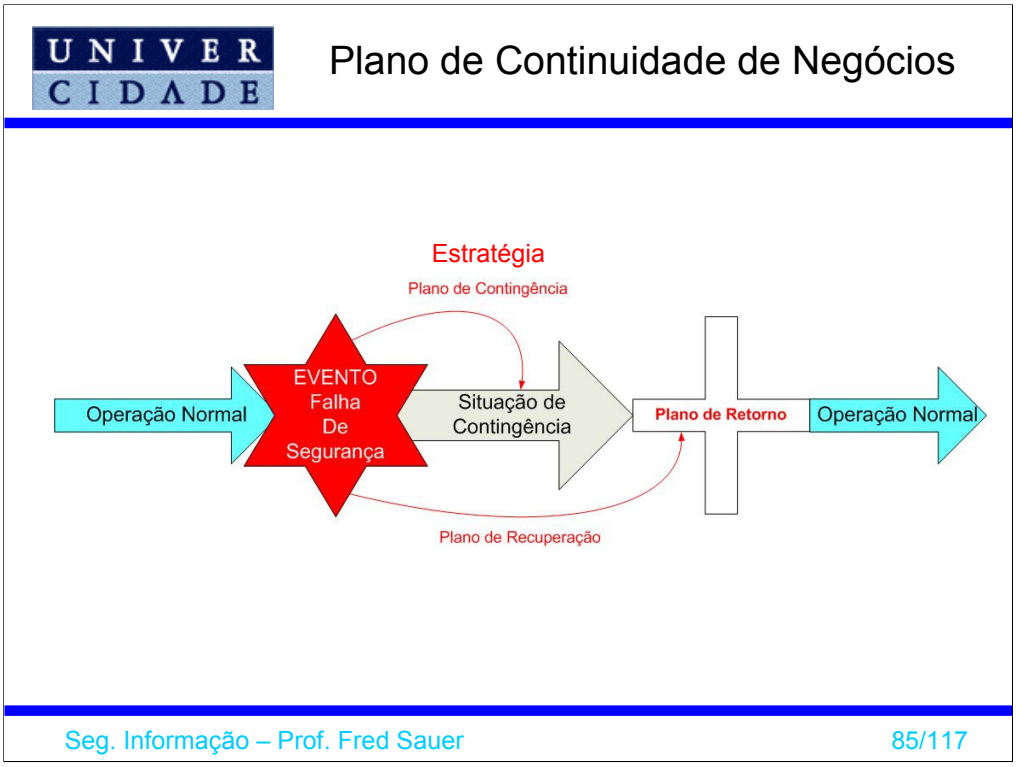
Plano de Continuidade de Negócios

- Deve ser elaborado com o objetivo de contingenciar situações e incidentes de segurança que não puderam ser evitados
- É composto por vários planos, focados em cada perímetro (físicos, tecnológicos, humanos) e com múltiplas ameaças potenciais
- Deve levar em conta a tolerância à falha de cada processo, e a resistência aos impactos
- Para cada objeto de contingência, deve ser selecionada a estratégia que melhor conduza o objeto a operar sob nível de risco controlado

O Plano de Continuidade dos negócios deve ser elaborado com o objetivo de garantir que todos os processos continuem suportando os processos vitais da empresa, levando-se em conta o tempo de recuperação no caso da ocorrência de um incidente de segurança. É formado pela análise de impactos no negócio, estratégias de contingência e 3 planos específicos: Plano de Administração de Crise (PAC), Plano de Continuidade Operacional (PCO) e Plano de Recuperação de Desastres (PRD).

É importante frisar que o objetivo deve ser sempre evitar a ocorrência de incidentes, e que o Plano de Continuidade visa apenas contingenciar as situações onde estes incidentes não puderam ser evitados.

Nenhuma empresa terá apenas um Plano de Contingências e sim vários planos focados em diferentes perímetros sejam eles físicos, tecnológicos ou humanos, e voltados para múltiplas ameaças potenciais. Essa segmentação é necessária porque há processos com tolerância à falhas variável, bem como extensões de impactos igualmente variáveis em gravidade, de forma que se deve selecionar as melhores estratégias para a operação sob um determinado nível de risco controlado.



Essa figura ilustra os papéis do Plano de Contingências, O Plano de Retorno e o Plano de Recuperação.

UNIVERCIDADE

Análise de Impactos - BIA

- Primeira etapa do Plano de Continuidade
  - Fornece informações para o dimensionamento das demais fases
  - Objetiva levantar o grau de relevância de processos e atividades
  - Permite mapear ativos e impactos que poderiam afetar a continuidade

Processos de Negócio / Escala		PN1	PN2	PN3	PN4	...	PNn
1	não considerável						
2	relevante	X					
3	importante			X			
4	crítico				X		
5	vital		X				

O BIA – *Business Impact Analysis* é um instrumento mundialmente conhecido que se destina a avaliar os impactos quantitativos que podem ser gerados com a paralisação total ou parcial de um determinado Processo de Negócio. Fornece informações para o perfeito e adequado dimensionamento do Plano de Continuidade. Com essa análise, pode-se definir prioridades de contingência, níveis de tolerância à indisponibilidade, agrupar os ativos de acordo com as suas similaridades. A figura a seguir ilustra a aplicação do BIA relacionada com as ameaças para o negócio, resultando num valor de tolerância para cada um dos PN ser contingenciado.

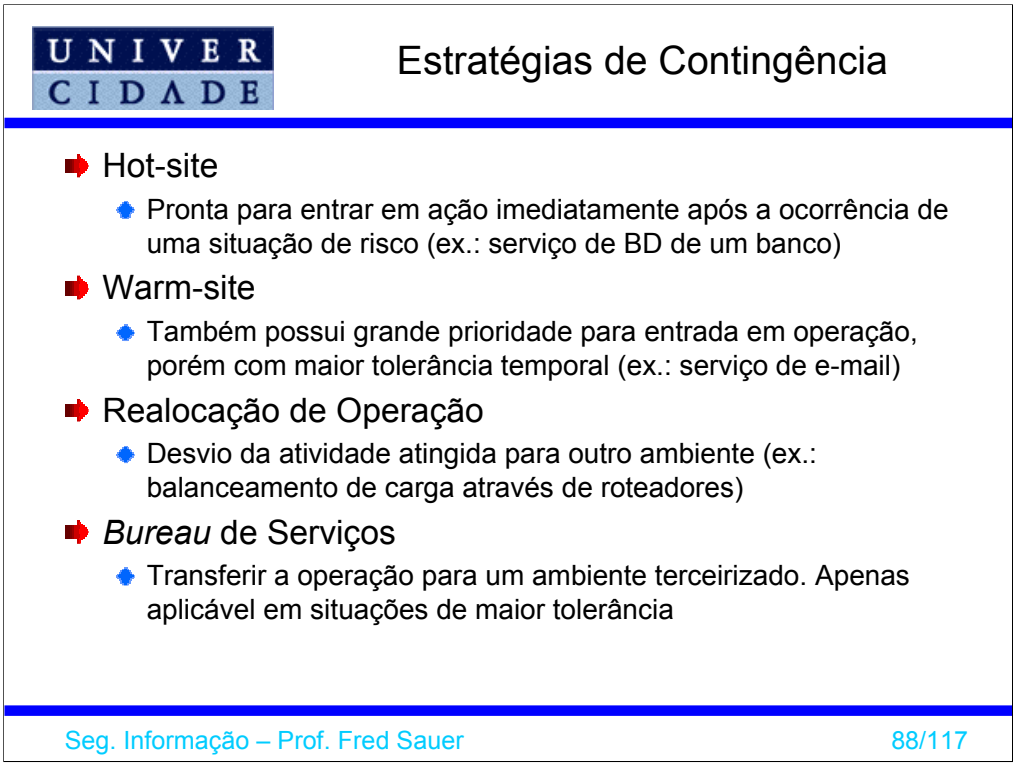
UNIVERCIDADE

Business Impact Analysis

- De posse do BIA, é possível priorizar as ações de contingência, os níveis de tolerância à indisponibilidade e agrupar ativos por similaridades
- Resta então definir as ameaças a contingenciar

Ameaças → / Processos de Negócio ↓	Incêndio	Greve	Falta de Energia	DoS	Sabotagem	...	Tolerância Temporal
Processo de Negócio 1	X		X		X		48h
Processo de Negócio 2	X						5h
Processo de Negócio 3	X	X	X	X			24h
Processo de Negócio 4				X	X		15min
Processo de Negócio n							

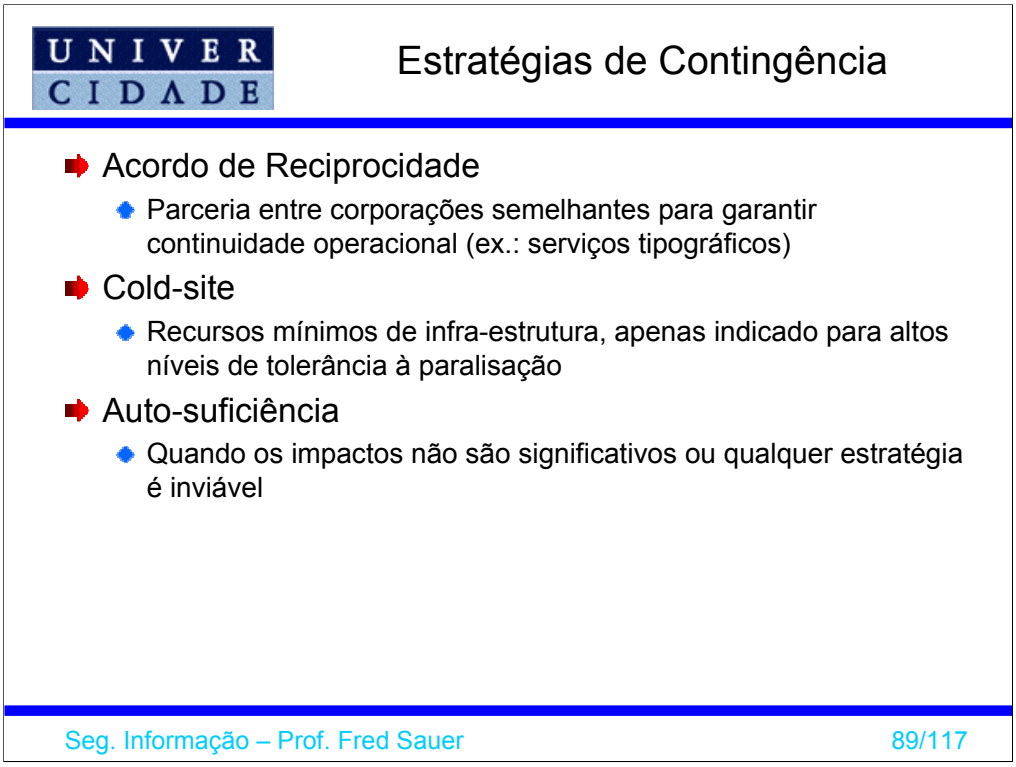
Essa tolerância se relaciona ao grau de criticidade de cada um dos PN.



Para cada nível de tolerância há estratégias passíveis de adoção. A ***Hot-site***, por exemplo, é a mais imediata e está sempre prestes a entrar em ação, oferecendo um tempo mínimo ou até inexistente de paralisação.

A ***Warm-site***, aplicável a situações menos exigências que a anterior porém ainda com baixa tolerância à paralisação, oferece soluções prontas para contingenciar incidentes, porém que implicam em alguma latência de implementação. Esse exemplo do e-mail ilustra uma situação warm-site, em que se pode usar enlaces alternativos para o despacho de mensagens, porém a necessidade de reconfiguração demandaria algum tempo a mais para retorno a operação. A **Realocação de Operação** prevê o desvio da atividade atingida por um incidente para outra instalação, ambiente físico, enlace, equipamento, pertencentes à mesma empresa e disponíveis. Essa estratégia implica em algumas questões: a primeira é a necessidade de redundância que demanda recursos, nem sempre disponíveis. Um bom exemplo é a disponibilidade de um segundo roteador em rede para implementação de redirecionamento de carga em caso de indisponibilidade.

O Bureau de serviços é semelhante ao anterior, porém com o uso de infra-estrutura terceirizada. Se por um lado dispensa a necessidade de se manter recursos redundantes, por outro traz inconvenientes como o manuseio das informações da empresa por terceiros e requerer maior tempo de tolerância.



O **Acordo de Reciprocidade** é interessante quando a implementação das estratégias de contingência se apresentassem inviáveis pelos altos custos. A aproximação entre empresas com características semelhantes (físicas, tecnológicas e humanas) visa uma alocação da atividade atingida nessa outra empresa, através do compartilhamento de recursos. Apesar do benefício do baixo custo, continua-se com o problema da manipulação dos dados por terceiros, agravado pelo fato que empresas com características semelhantes tipicamente são concorrentes. Um exemplo é a impressão da tiragem de jornais.

A estratégia ***Cold-site*** propõe uma alternativa viável apenas para instalações sem recursos de processamento de dados e recursos mínimos de infra-estrutura e telecom, ficando à mercê de soluções que serão implementadas para cada caso, de acordo com a disponibilidade de recursos e pessoal.

A **auto-suficiência** é o extremo oposto da hot-site, e é aplicável quando nenhuma das estratégias anteriores é adequada, ou porque os impactos não são significativos ou então estas estratégias não são economicamente viáveis.

Os Planos de Contingência são desenvolvidos de acordo com cada uma das ameaças para cada um dos PN relevantes e críticos, definindo detalhes operacionais para cada um dos incidentes de segurança possíveis. É dividido em 3 módulos distintos e complementares que tratam especificamente de cada momento vivido pela empresa.

O **Plano de Administração de Crises (PAC)** – Define o passo-a-passo do funcionamento das equipes envolvidas com o acionamento das contingências, antes, durante e depois do incidente. Também define procedimentos que devem ser realizados quando a empresa voltar à normalidade. Um exemplo é a estratégia de comunicação do fato ocorrido à imprensa. É o mais genérico.

O **Plano de Continuidade Operacional (PCO)** – Define os procedimentos para o contingenciamento dos ativos que suportam cada um dos PN, para redução do tempo de indisponibilidade e conseqüentemente, a extensão dos impactos provocados pelo incidente. Um exemplo é a definição de ações a tomar no caso da queda de uma conexão com a Internet. É objetivamente focado nos ativos.

O **Plano de Recuperação de Desastres (PRD) -** Objetiva definir procedimentos de recuperação e restauração das funcionalidades dos ativos aos níveis originais de operação.

É fator crítico de sucesso definir precisamente os gatilhos para acionamento destes planos. estes gatilhos são tipicamente parâmetros de tolerância, que se ultrapassados estão inferindo em perdas (impactos) para o negócio, e definidos através do BIA. Podem também ser usados outros parâmetros, como o percentual do recurso afetado, perdas financeiras, etc.

Este modelo deve ser dinâmico, testado e ajustado periodicamente para garantir a sua eficácia.

Plano de Continuidade - Conclusões

- É complexo por abranger diversos objetos com características personalizadas e dinâmicas, várias ameaças e necessidade da perfeita integração dos seus componentes
- Tem importância vital por ser a última camada de segurança
- Por conta disso, deve ser periodicamente submetido a testes e simulações de funcionamento, que também permitirão a realização de ajustes dinâmicos

O Plano de Contingências é um elemento que é planejado para ser executado apenas em último caso, ou seja após todas as precauções de segurança disponíveis terem falhado. Por conta disso, é comum que o mesmo seja pouco utilizado, caindo em obsolescência se não for permanentemente testado e atualizado, para que seja eficaz quando necessário.

UNIVERCIDADE

Estudo de Caso – Parte 3

- Análise BIA
- Definição de Estratégias de Contingência
- Planos de Continuidade do Negócio

UNIVERCIDADE

Análise BIA

	Candidato	Sabotador	Pane Elétrica	Técnico	Tolerância
PN1	X				20 dias
PN2		X	X	X	2 horas

UNIVER CIDADE

Plano de Continuidade

Plano de Administração da Crise (PAC) – O responsável pela administração desta contingência é o Gestor de TI. Na sua ausência, o funcionário hierarquicamente mais graduado deve assumir as ações deste plano. O gestor de TI da empresa (ou o seu substituto), verifica a característica da interrupção (extensão da interrupção, possíveis razões internas e externas), registra a ocorrência (horário e dados verificados) e determina a um funcionário do setor de TI que comunique ao Diretor de Operações a ocorrência. O gestor de TI verifica a desobstrução do local onde os geradores de emergência contratados eventualmente ficarão operando;

O Plano de Continuidade Operacional (PCO) – Deve focar na tolerância do PN. Para garantia de continuidade do ERP, primeiramente o Gestor de TI deve acionar a empresa conveniada de fornecimento de geradores e colocá-la de sobreaviso para o atendimento da ocorrência em questão. Entra em contato com a empresa de fornecimento de energia e busca informações sobre uma estimativa de retorno. Caso não haja previsão, solicita à empresa de geradores que mande os equipamentos. Caso contrário, aguarda até uma hora de interrupção antes de solicitar os geradores.

Tão logo os geradores cheguem à empresa, o Gestor de TI recebe os técnicos, orienta quanto ao local de instalação, determina seu acionamento imediato e coordena a manobra de entrada em operação do mesmo, até que substitua os no-break da estrutura de contingência;

O Plano de Recuperação de Desastres (PRD) – Tem uma importância fundamental no Plano de Contingências, porque visa a avaliação da eficiência e a eficácia dos controles, de forma a evitar que novas ocorrências reduzam a capacidade operacional do recurso contingenciado. Assim, são eventos importantes no PRD em questão – análise dos parâmetros da ocorrência: tempo de paralisação, razões evidenciadas, e, principalmente, estimativa de prejuízos com a paralisação. Avaliação preliminar do SLA. Encaminhamento para o setor jurídico, visando o ressarcimento dos prejuízos. Na próxima reunião com o comitê Gestor de Segurança da Informação, discutir a viabilidade da reavaliação da autonomia do sistema de no-break de cada um dos componentes, um SLA mais rigoroso com a operadora e um contrato diferenciado com a empresa dos geradores. O objetivo sempre é a manutenção do nível de risco sob controle.

UNIVER CIDADE

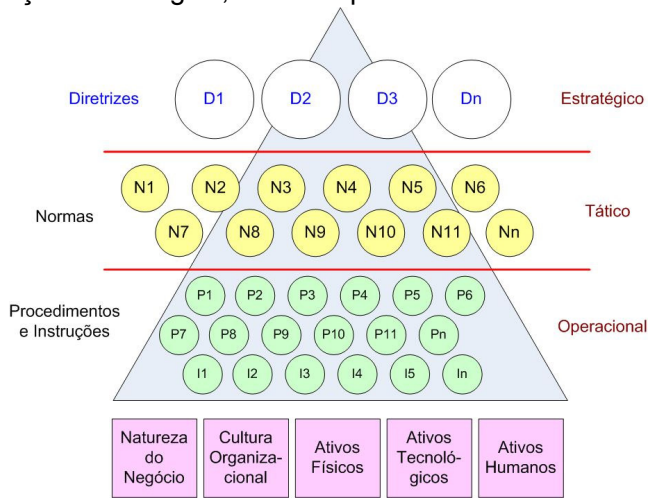
Conclusões desta Fase

- Esta fase descreve mecanismos de contingência para manter os PN em operação MESMO na presença de ameaças em ação;
- É importante observar que o objetivo AQUI não é evitar os incidentes, e sim os seus efeitos (impactos)

UNIVER CIDADE

Política de Segurança da Informação

- Subdividida em blocos adequados para cada um dos níveis da organização: Estratégico, tático e operacional



Seg. Informação – Prof. Fred Sauer 96/117

A Política de Segurança da Informação não um manual de procedimentos. É um conjunto de diretrizes, normas, procedimentos e instruções de grande abrangência, que se destinam a implementar e garantir o controle do nível de risco para a corporação. Seus objetivos são destinados a todos os setores da empresa, porém os documentos são direcionados para cada um dos setores, estratégico (executivo), tático e operacional, estabelecendo padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações de acordo com o nível de segurança estabelecido sob medida para a empresa. A Política de Segurança, então, é altamente particularizada para cada empresa.

As Diretrizes tem papel estratégico, expressando a importância que a empresa dá para a informação, além de comunicar aos seus funcionários seus valores e o seu comprometimento com os desafios de se incrementar a segurança na cultura organizacional. Por ser um conjunto de documentos da alta direção da empresa, serve como norteador das atividades táticas e operacionais. Definem responsabilidades dos elementos manipuladores da informação, estrutura do *Security Office*, métricas, índices e indicadores, controles de conformidade, requisitos de capacitação de usuários, mecanismos de controle de acesso físico e lógico, responsabilizações, auditoria do uso de recursos, registro de incidentes e gestão de continuidade do negócio.

As normas são usadas no nível tático para detalhas situações, ambientes, processos específicos e fornecendo orientação para o uso adequado das informações. São naturalmente mais numerosas do que as diretrizes. Critérios para admissão e demissão, criação e manutenção de contas e senhas de usuários, descarte de informações, desenvolvimento e manutenção de sistemas, uso da internet, acessos remotos, notebooks, pendrives e câmeras digitais. Contratação de terceiros e classificação da sensibilidade da informação são bons exemplos de normas.

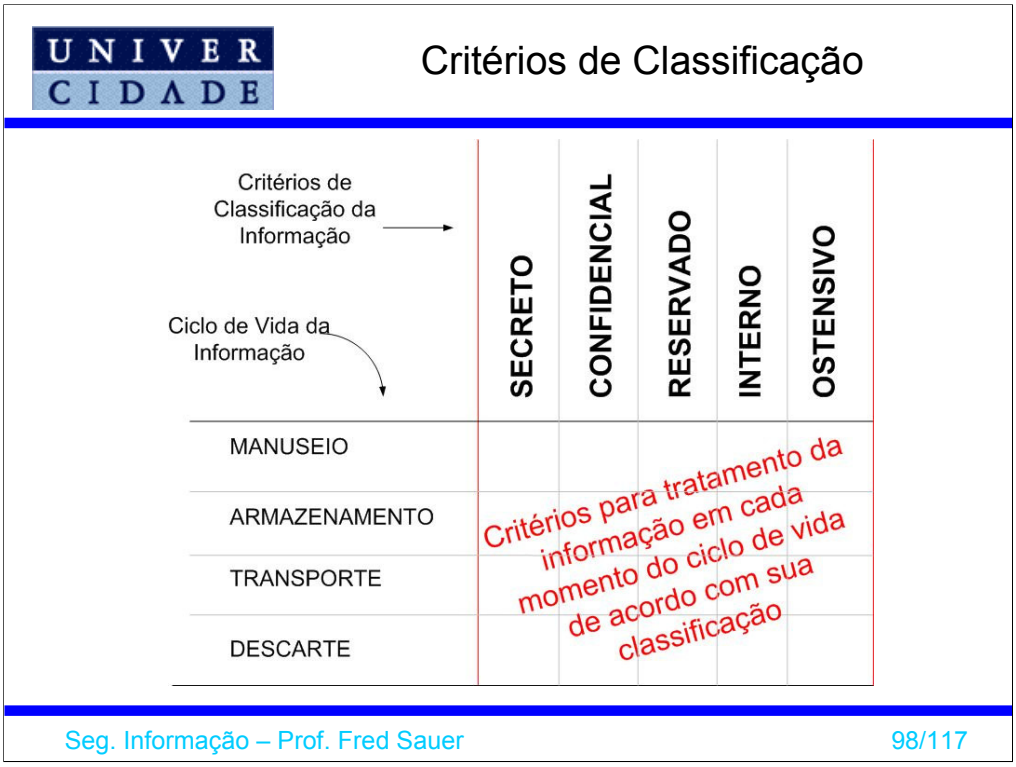
Procedimentos e Instruções aplicáveis ao nível operacional são bem mais numerosas e devem descrever meticulosamente cada uma das ações e atividades relacionadas com o uso das informações. Um bom exemplo é: enquanto a diretriz orienta estrategicamente para a necessidade de salvaguardar informações sigilosas, a norma define que as mesmas devem ser criptografadas com ferramentas de acordo com o grau de sigilo, e os procedimentos e instruções descrevem os passos necessários para executar tal criptografia caso-a-caso.

UNIVER CIDADE

Política de Segurança da Informação

- Estabelece padrões, responsabilidades e critérios para todo o ciclo de vida da informação, de acordo com o nível estabelecido pela empresa → por isso é essencialmente personalizada
- **Diretrizes** – Papel estratégico. É a comunicação formal da empresa sobre a importância dada à informação, definindo linhas de ação (ex.: atribuição de responsabilidades, controles de conformidade, métodos de acesso físico e lógico, auditoria, registro de incidentes, etc.)
- **Normas** – Caráter Tático. Abrange maior especificidade nos processos, situações e ambientes, detalhando as diretrizes para cada caso (ex.: critérios para admissão e demissão, criação e manutenção de senhas, uso da Internet, classificação das informações, etc.)

Para elaborar uma PolSeg, deve-se iniciar pela elaboração das diretrizes, envolver os executivos e conquistar apoio. Estabelecer responsáveis e gestores diretos pela manutenção da PolSeg. Elaborar um programa de divulgação das diretrizes, normas, procedimentos e instruções, como instrumento de disseminação da cultura e conscientização do pessoal. Buscar sempre o envolvimento de todos os funcionários, de forma a agregar responsabilidade pela continuidade do negócio, principalmente pela responsabilidade específica sobre as informações sob sua custódia.



Essa figura ilustra a relação entre classificação e tratamento definido na Política para o Ciclo de Vida da Informação. Para isso, é preciso entender profundamente o perfil do negócio e as características das informações que alimentam os processos e circulam no ambiente corporativo, para que os critérios sejam personalizados.

UNIVER CIDADE

Política de Segurança da Informação

- Procedimentos e Instruções
  - Descrição meticulosa de cada ação
  - Exemplo:
    - ✓ A **Diretriz** determina como estratégico a salvaguarda de assuntos sigilosos
    - ✓ A **Norma** define que assuntos sigilosos definidos por um determinado critério devem ser criptografado
    - ✓ O **Procedimento** descreve passo-a-passo como criptografar o arquivo
- Conclusões:
  - O processo deve ser *top-down* (iniciar pelas diretrizes)
  - Os executivos devem estar envolvidos e motivados
  - A ampla divulgação é fundamental
  - O funcionário também deve ser envolvido e motivado

UNIVER CIDADE

Estudo de Caso – Parte 4

- Política de Segurança da Informação

UNIVER CIDADE

Política de Segurança

DIRETRIZ – Por ser um recurso de grande importância para a organização, a confidencialidade das informações deve ser preservada de acordo com o seu controle de acesso e seu sigilo..
NORMA – Cada setor deve ter definido o seu controle de acesso, seus perímetros de segurança e regras específicas para acesso (ou não) de público externo. No caso específico do setor de Gestão do ERP, podemos definir: O acesso de elementos estranhos à empresa apenas deverá ser feito nas seguintes condições: Divulgação de produtos e serviços – apenas as quartas e sextas, das 14h às 15hs, mediante agendamento com o Gestor do PN; Manutenção de equipamentos, infra-estrutura e aplicativos – mediante cadastramento e acompanhamento permanente de um funcionário do setor, em data e horário previamente acertado com o Gestor; e Visita de parentes de funcionários ao setor – vedadas.
PROCEDIMENTOS – Para a realização de manutenções no setor, a empresa prestadora deverá enviar os dados dos funcionários previamente (RG, função, tarefa a cumprir). Os dados serão verificados na chegada do prestador de serviços, que será orientado a não circular em nenhum momento pela empresa desacompanhado. Receberá um crachá RFID com permissão de acesso apenas aos setores rigorosamente necessários e aos banheiros. Será notificado que a empresa é monitorada por câmeras e alarmes de acesso a áreas restritas. Será informado que isto ocorrendo, ele será obrigado a retirar-se e a empresa será notificada de seu procedimento. Um colaborador da empresa será indicado pelo gestor para acompanhar o prestador de serviço durante toda a sua permanência na empresa. Após a realização do serviço, o prestador será acompanhado até a portaria pelo colaborador responsável. O registro de sua presença será mantido para eventuais perícias futuras.

UNIVERCIDADE

Conclusões desta Fase

- Aqui são descritos os mecanismos de controle nas áreas física, tecnológica e humana;
- A PS deve ser dinâmica e acessível;
- Deve ser o norteador das ações de disseminação da cultura da SegInfo

Análise de Riscos e Vulnerabilidades

- É o diagnóstico fundamental da situação de segurança da empresa
- Duas linhas metodológicas:
  - Quantitativa – mensura os impactos à partir do valor do ativo
  - Qualitativa – mensura estimativamente os impactos no negócio como um todo. É mais eficiente pela consideração do valor subjetivo do impacto
- Aspectos considerados na Análise de Riscos
  - Relevância de um processo para o negócio
  - Dependência entre processos e ativos
  - Projeção de impactos
  - Probabilidade da exploração de uma ameaça
  - Severidade potencial de exploração de um ativo
  - Qualificação das vulnerabilidades e das ameaças

Por ser um procedimento crítico de sucesso para a SegInfo, a Análise de Riscos deve ser bem compreendida e corretamente executada. A maioria das iniciativas tende a concentrar o mapeamento de vulnerabilidades principalmente nos ativos tecnológicos, o que não é suficiente para diagnosticar com precisão os reais riscos que envolvem a operação da empresa. Processos, ambientes físicos, pessoas, sistemas, informações e equipamentos são pilares que sustentam os processos de negócio e conseqüentemente o próprio negócio. Há também variáveis exógenas que influenciam o nível de risco, como por exemplo as ameaças que surgem em função de mudanças estratégicas.

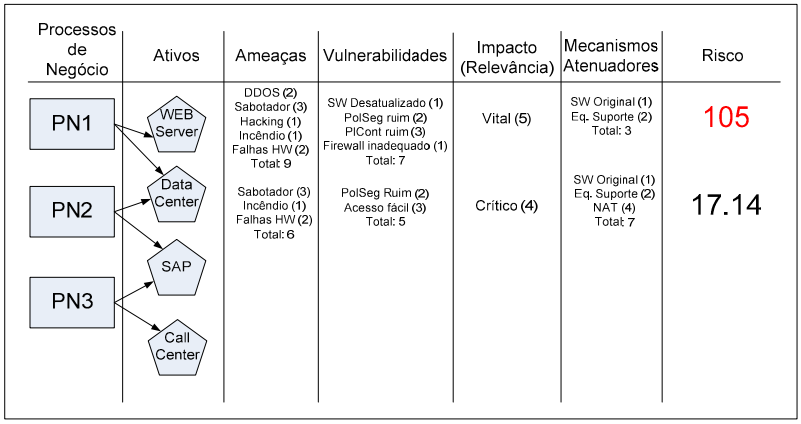
A Análise de Risco, portanto deve ser ampla e focada no negócio como um todo. Pode seguir a linha quantitativa, orientada a mensurar os impactos financeiros provocados por um incidente de segurança, calculado à partir do valor dos próprios ativos. A linha qualitativa usa critérios para estimar os impactos de um incidente de segurança causado por uma ameaça, mas tem uma componente mais subjetiva do que a quantitativa, permitindo a contabilização do aparentemente intangível.

Aplicando-se a metodologia para mapeamento de processos de negócio adotada no PDS, ou até mesmo “herdando” os resultados dessa atividade, tem-se o mapa de relacionamento e dependência dos ativos. Coleta-se evidências e identificação de ameaças e vulnerabilidades dos ativos, para o cálculo de risco.

UNIVERCIDADE

Análise de Riscos e Vulnerabilidades

- Estes aspectos permitem a construção de um mapa de relacionamento com situações de causa e efeito.



Com a lista apresentada no *slide*, monta-se o mapa de relacionamento com a projeção de situações de causa e efeito, com ligações múltiplas, pontuações e qualificação de ameaças e vulnerabilidades, associadas a estudos de probabilidades e impactos que tornar-se-ão elementos subsidiadores do cálculo do risco.

A identificação de ameaças e vulnerabilidades é feita através de instrumentos como entrevistas, inspeção física e de documentos, análise técnica de ativos tecnológicos através de normas de certificação (EIA/TIA 568A), software especializado para varredura e *scanning*.

UNIVERCIDADE

Análise de Riscos e Vulnerabilidades

- As atividades de coleta de evidências são suportadas por metodologias e instrumentos de apoio, como a EIA/TIA 568, *scanners*, e, principalmente, uma base de conhecimento atualizada
- Obtidos os riscos, pode-se organizar as prioridades, definir planos de ação de curto, médio e longo prazos, modelar contramedidas para cada perímetro, definir o nível de risco desejável
- Segurança é administrar um nível aceitável de risco

O nível de risco de um determinado PN é projetado à partir do nível de risco de cada ativo que o sustenta. O resultado permite a definição de prioridades, dimensionar plano de ação de curto médio e longo prazos, de acordo com o nível de risco de cada um.

Pelo menos no início, convém alinhar os resultados da análise de riscos aos controles sugeridos pela norma ISO 17799 e identificar o nível de conformidade atingido pela empresa através da medição da aderência a cada um dos 127 controles de segurança.

UNIVERCIDADE

Análise de Riscos e Vulnerabilidades

- Teste de Invasão
  - Papel complementar na análise das vulnerabilidades. Simula tentativas de acesso indevido para avaliar o grau de segurança
  - A qualidade do teste não está ligada aos resultados, mas à similaridade com as práticas reais
  - Formatos
    - ✓ **Interno** – Simula ataques por funcionários da própria empresa ou terceirizados de dentro do ambiente interno
    - ✓ **Externo** – Usa recursos de acesso remoto
    - ✓ **Cego** – Realizado na ausência completa de informações privilegiadas que facilitam os ataques. Válido por testar a cultura do ativo humano com o uso de técnicas de Engenharia Social
    - ✓ **Não-cego** – Usa informações privilegiadas, tipicamente disponíveis para funcionários da empresa
  - Deve ser executado apenas por profissionais qualificados e de acordo com uma metodologia

O Teste de Invasão deve aproximar-se ao máximo das técnicas reais. Deve simular ataques internos e externos, cegos e não-cegos. O teste do teste cego é a aplicação da Engenharia Social, e com a obtenção das informações necessárias, realizar o não-cego. Para dar credibilidade e importância aos resultados que serão obtidos, recomenda-se que os testes de invasão sejam realizados apenas após a aprovação do corpo executivo. Para aprovação, um planejamento deve ser submetido, prevendo todas as etapas, desde a preparação e definição da equipe e ferramentas, até a elaboração de relatório detalhado.

UNIVERCIDADE

Implementações de Controles

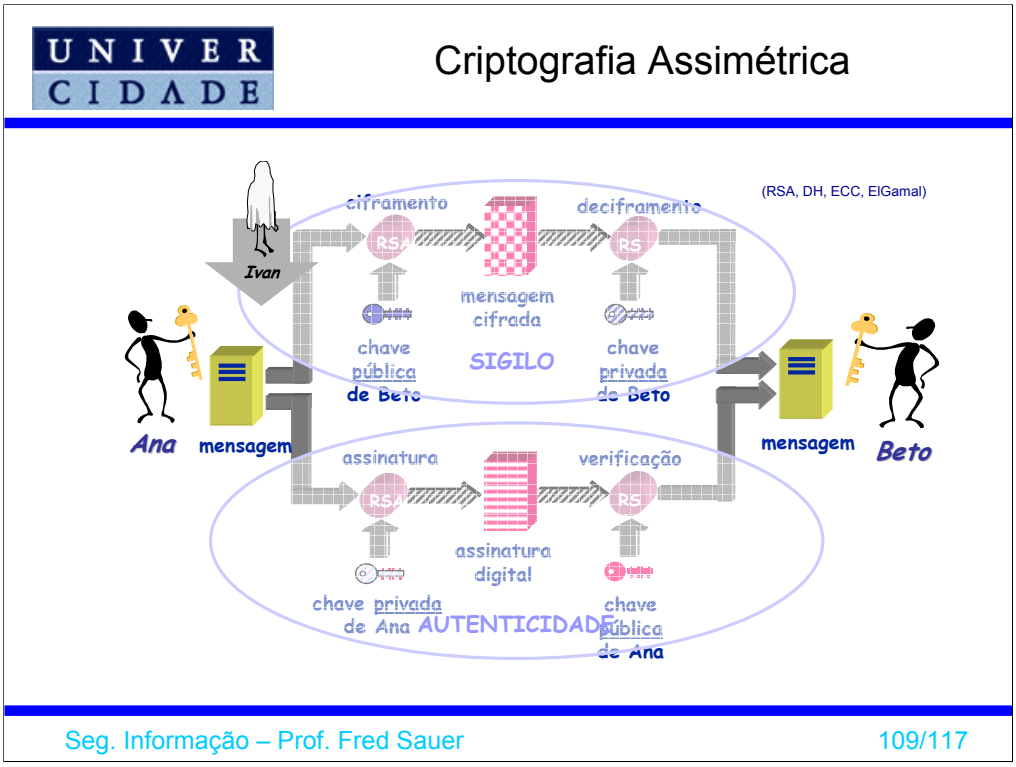
- Voltados ao *Peopleware*:
  - Estratégia de capacitação
  - Procedimentos contratuais diversos
  - Auditorias
  - Monitoramento e filtragem de conteúdo
  - Termos de responsabilidade, etc.
- Direcionados ao ambiente físico
  - Controles físicos de acesso
  - Cabeamento estruturado
  - Fragmentadoras
  - Sistemas de Backup
  - Nobreak, estabilizadores, etc.

Como se disse anteriormente, o macro-desafio da segurança é controlar o nível de risco. As providências acima contribuem muito mais para esse controle do que qualquer política de restrições e proibições.

UNIVER CIDADE

Implementações de Controles

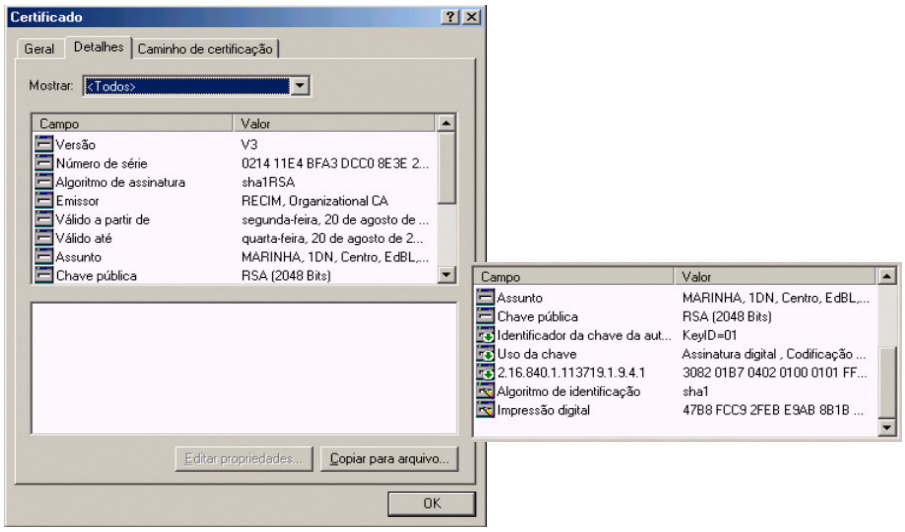
- Controles aplicáveis aos ativos tecnológicos
  - Autenticação e autorização – condizentes com os direitos
    - ✓ O que você sabe
    - ✓ O que você tem
    - ✓ O que você é
  - Combate a Ataques e Invasões – SW e HW especializado
    - ✓ Firewall
    - ✓ Detector de Intrusos
  - Privacidade das Comunicações
    - ✓ Criptografia Simétrica
    - ✓ Criptografia Assimétrica e Certificados Digitais
    - ✓ *Virtual Private Networks – VPN*
    - ✓ Public Key Infraestructure – PKI (ICP)



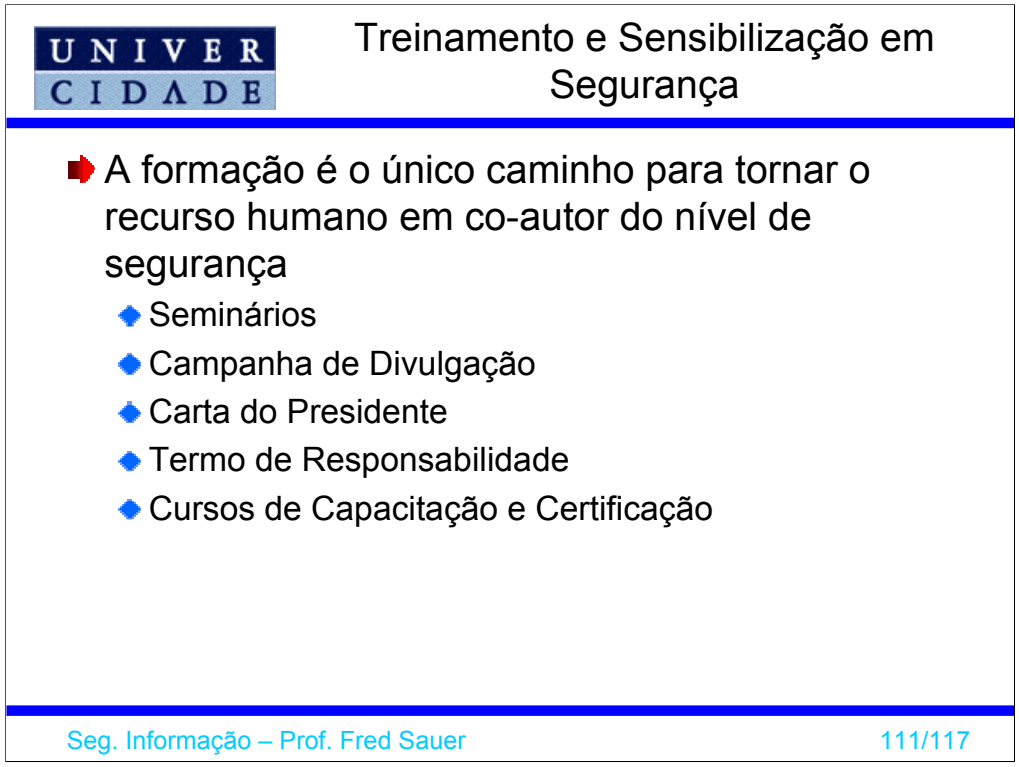
Essa figura ilustra as duas formas de se utilizar a criptografia Assimétrica. O uso de um par de chaves, com uma parte pública e a outra privada, pode-se obter dois aspectos de segurança objetivamente: A Confidencialidade, quando utilizamos a chave pública do destinatário para criptografar a mensagem, pois apenas a sua chave privada poderá transformar esse criptograma em texto claro. Usando-se, por sua vez, a chave privada do emissor para criptografar a mensagem, garante-se a Autenticidade, pois qualquer pessoa poderá decifrá-la através da componente pública da chave, mas a consecução dessa operação com sucesso garantiu que apenas o detentor da chave privada correspondente poderia ter criado o criptograma. Outro aspecto obtido indiretamente é a Integridade, porque um criptograma alterado nunca mais poderá ser decifrado.

UNIVERCIDADE

Certificado Digital



Esse é um exemplo de Certificado Digital. Tais documentos conduzem uma série de informações que possibilitam a utilização de algoritmos simétricos e assimétricos, podendo pertencer à pessoas físicas ou jurídicas. Será um elemento obrigatório para transações no futuro, e demandará a substituição dos cartórios tradicionais para digitais.



Atividades informativas e de congregação de esforços em torno da Segurança contribuem significativamente para a conscientização do elemento humano.

UNIVER CIDADE

Equipe para Resposta a Incidentes

- Construção de um modelo para oferecer eficiência e grande velocidade na resposta a incidentes, seja com recursos próprios ou terceirizados
- Coordenada pelo *Security Officer*

Essa equipe deve ser dimensionada de acordo com as necessidades mapeadas em etapas anteriores.

UNIVER CIDADE

Administração e Monitoração de Segurança

- Observação dos desvios de conduta, sobrecarga da infra-estrutura, tentativas de ataques e invasão, ineficiência dos controles implementados e, principalmente, mudanças físicas, tecnológicas e humanas que provoquem oscilações do nível de segurança
- A auditoria faz parte deste processo
- Logs e Registro de ocorrências

Sem um processo dinâmico e perseverante de acompanhamento da eficiência dos controles não é possível a adoção da confortável postura pró-ativa.

Estudo de Caso – Parte Final

- Planejamento da Análise de Riscos

UNIVER CIDADE

Análise de Riscos

Auditoria de Conformidade – Os controles previstos na política de segurança são testados, através de entrevistas verificando se os gestores estão capacitados para a condução dos procedimentos previstos, bem como se conhecem as normas pertinentes aos seus setores e as diretrizes do setor executivo. Os documentos de controle são verificados (planilhas de exercícios de capacitação, históricos de entrada em operação dos PLCONT, registros de incidentes de segurança, registros de testes com os Planos de Contingência, etc.), e todas as discrepâncias são registradas;

Auditoria de Rigidez Física – São feitas verificações da rigidez dos controles de acesso, da infra-estrutura, dos perímetros de segurança, dos controles de manutenção de hardware (inventários, MTBF, manutenção preventiva), SLAs de prestadoras, contratos de manutenção em vigor, verificação de *gaps* para descrição em relatório;

Auditoria de Rigidez Lógica – Os Sistemas Operacionais em uso são testados com relação à sua atualização (inclusive os de equipamentos de conectividade). As aplicações são verificadas quanto a vulnerabilidades conhecidas e aleatórias, como por exemplo no transporte de informações sigilosas de forma não criptográfica. Os controles lógicos (Firewall, IDS, antivírus corporativos) são testados e verificados com ferramentas especialistas de ataque; e

Auditoria de Capacitação – São usadas técnicas de Engenharia Social para verificar o nível de mentalidade de segurança entre os colaboradores da empresa; são evidenciadas as principais deficiências de forma genérica, sem apontar nomes, para sugestão de estratégias na capacitação do pessoal.

UNIVERCIDADE

Análise de Riscos

- Ações Genéricas:
  - Reuniões com os Gestores para verificação dos modelos em vigor
  - Ações de testes dos Planos de Continuidade
- Ações Específicas:
  - Auditorias de Conformidade com a PS em vigor
  - Ações de Engenharia Social buscando acesso à informação crítica
  - Ações técnicas com o uso de ferramentas buscando acesso à informação crítica
  - Ações de Análise pró-ativa de *logs*, alarmes de bloqueios bem sucedidos e relatórios de IDS e IPS

UNIVER CIDADE

Conclusões desta Fase

- Como importante ferramenta para o PDCA, é importante que os resultados obtidos resultem em alterações no Planejamento e nos Controles (fase *Act*)