Segurança da Informação

Frederico Sauer, D.Sc.
Auditor de Segurança da Informação
fsauer@gmail.com

Objetivos Essenciais

- Conceito de Risco e suas componentes
- Mensurabilidade do Risco
- Gestão do Risco
- Elementos para identificação de riscos
- Atributos da Informação
- *Security Office* e FSI (ou CGSI)
- Plano de Continuidade (PAC, PCO e PRD)
- Política de Segurança (Diretrizes, Normas e Procedimentos)

Conceito

- Por quê investir em Segurança ?
- Qual é o significado de Risco ?
  - RISCO
    - Ameaças
    - Vulnerabilidades
    - Impactos
  - CONTROLES
    - Mecanismos para reduzir o Risco

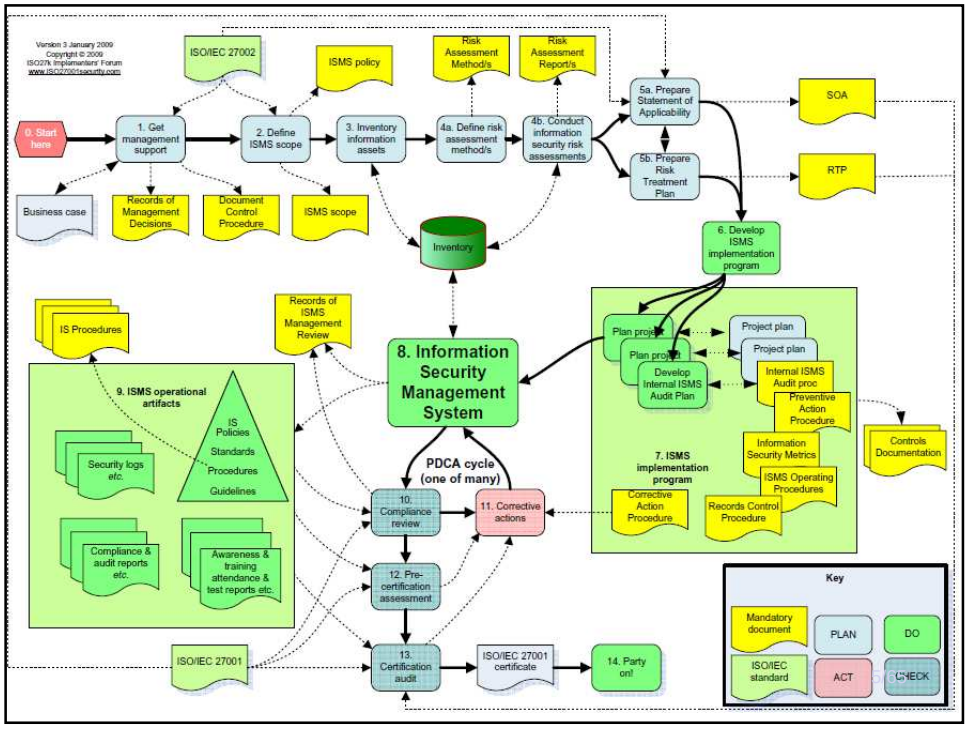
$$R = \frac{V \times A \times I}{M}$$

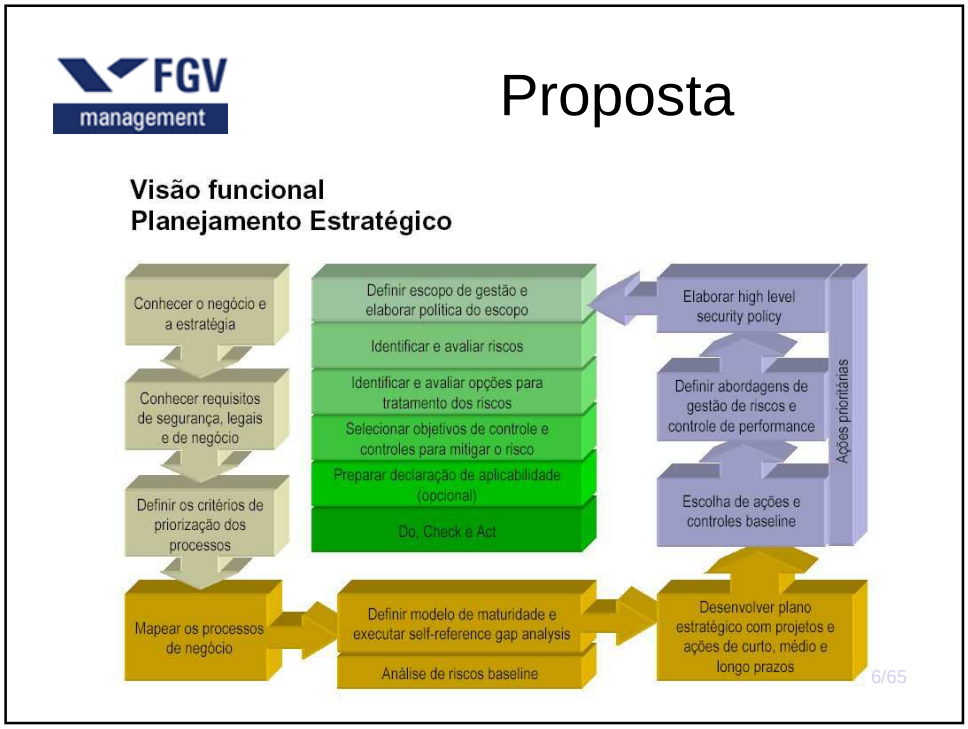
3/65

Risco

- O que são ameaças ?
- O que são vulnerabilidades ?
- Quão impactante pode ser um Incidente de Segurança ?
- Como podemos controlar este risco ?

4/65


Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com
ISO/IEC 27002
ISMS policy
Risk Assessment Method/s
Risk Assessment Report/s
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4a. Define risk assessment method/s
4b. Conduct information security risk assessments
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
SOA
RTP
Business case
Records of Management Decisions
Document Control Procedure
ISMS scope
Inventory
6. Develop ISMS implementation program
IS Procedures
Records of ISMS Management Review
8. Information Security Management System
9. ISMS operational artifacts
IS Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
PDCA cycle (one of many)
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
ISO/IEC 27001
ISO/IEC 27001 certificate
14. Party on!
Plan project
Plan project
Develop Internal ISMS Audit Plan
Project plan
Project plan
Internal ISMS Audit proc
Preventive Action Procedure
Information Security Metrics
ISMS Operating Procedures
Records Control Procedure
Corrective Action Procedure
7. ISMS implementation program
Controls Documentation
Key
Mandatory document
ISO/IEC standard
PLAN
DO
ACT
CHECK


FGV
management
Proposta
Visão funcional
Planejamento Estratégico
Conhecer o negócio e a estratégia
Conhecer requisitos de segurança, legais e de negócio
Definir os critérios de priorização dos processos
Mapear os processos de negócio
Definir escopo de gestão e elaborar política do escopo
Identificar e avaliar riscos
Identificar e avaliar opções para tratamento dos riscos
Selecionar objetivos de controle e controles para mitigar o risco
Preparar declaração de aplicabilidade (opcional)
Do, Check e Act
Definir modelo de maturidade e executar self-reference gap analysis
Análise de riscos baseline
Elaborar high level security policy
Definir abordagens de gestão de riscos e controle de performance
Escolha de ações e controles baseline
Ações prioritárias
Desenvolver plano estratégico com projetos e ações de curto, médio e longo prazos
6/65

Proposta

- Metodologia prática:
  - Comportamento humano típico
    - Adere apenas ao que concorda
    - Concorda com o que lhe dê vantagens
    - Reage a mudanças abruptas, mas se adapta a novos ambientes que lhe pareçam favoráveis
  - Passo-a-passo metodológico:
    - Conhecimento
    - Envolvimento
    - Comprometimento

7/65

Fases

- 1ª fase → mapeamento do negócio
  - Conhecer detalhadamente o fluxo de informações
- 2ª fase → mapeamento dos ativos
  - Conhecer as relações entre ativos e informação
- 3ª fase → Análise de Riscos Baseline
  - Evidenciar situações de risco visíveis para todos

8/65

Fases (cont)

- 4ª fase → Análise CIDAL e GUT dos Processos
  - Foco total no negócio
- 5ª fase → Montagem de uma estrutura
  - Security Office e FSI
- 6ª fase → Elaboração de um PCN
  - Priorizado para os maiores riscos
- 7ª fase → Elaboração de uma PolSeg
  - Top-down
  - Inicia-se pelas Diretrizes
  - Abordagem objetiva à luz das fases 1 a 3

Mapeamento do Negócio

- Visão Holística do Risco
- Identificação de Influências
- Orientação básica
  - Evitar a visão míope
  - Foco na Informação
  - Ilustrada pelos gestores (a situação “real”, e não “a desejada”)

Objetivo do Mapeamento

- Isolar o fluxo de informações
- Identificar dependências funcionais entre os Processos
- Ferramenta de verificação de conformidade com a realidade
- Não deve “supor” ou “corrigir” neste momento

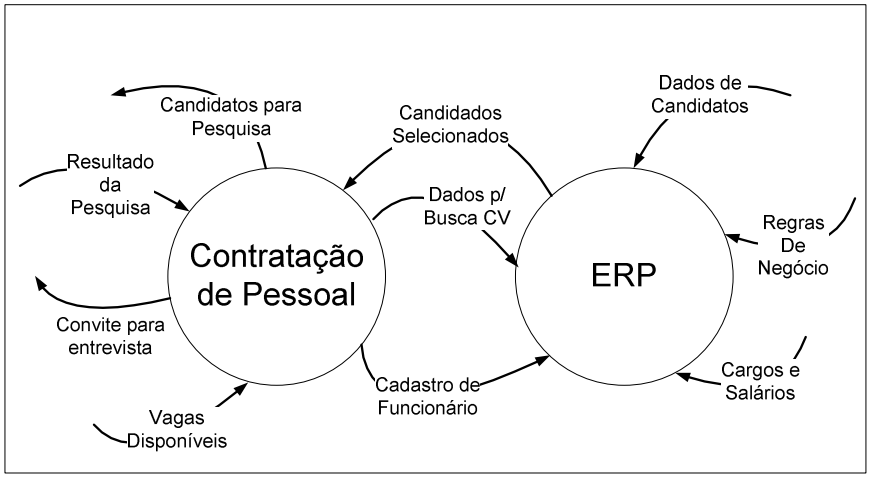
11/65

Caso

- Identificação e mapeamento dos Processos de Negócio do Estudo de Caso
- Trata-se de uma empresa de segurança patrimonial, onde a imagem é dependente do comportamento de seus colaboradores.

12/65

Resultado



Atividade

- Identificação e mapeamento de um processo de negócio do seu dia-a-dia (ex.: pagamento de contas via *Personal Banking*)

Segundo Passo

- Mapeamento de Ativos
  - Significado
  - Taxonomia
    - Físicos
    - Tecnológicos
    - Humanos

15/65

Segundo Passo

- Ciclo de Vida da Informação
  - Manipulação
  - Armazenamento
  - Transporte
  - Descarte

16/65

Objetivo desta etapa

- A correlação entre os ativos, informações e fase o ciclo permite:
  - Identificar controles apropriados à natureza do ativo
  - Planejar treinamentos apropriados
  - Proteger a informação em todo o seu ciclo de vida, através dos ativos
  - Evitar investimentos inadequados para os reais riscos

17/65

Caso

- Elaboração do quadro para o Estudo de Caso

18/65

Resultado (Extrato)

Ativo		Fase Ciclo	Info
PN Contratação de Pessoas	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

Atividade

- Fazer o segundo passo para o seu Processo de Negócio

Terceiro Passo: Análise de Riscos Baseline

- Principais Riscos
  - Casos Reais já ocorridos
  - Estatísticas com empresas semelhantes
  - Observação especialista
- Busca o envolvimento

21/65

Objetivos da Análise de Riscos Baseline

- Incidentes já ocorridos tem grande probabilidade de voltar a ocorrer
- Ainda não conhecemos o problema o suficiente
- A aderência à Política será favorecida pelo envolvimento
- Inicia-se um processo de aculturamento

22/65

Caso

- Análise de Riscos *baseline* do Estudo de Caso

LIBERAL notícias esportes entretenimento mu

NOTICIAS / BRASIL

10/04/2013 13:29 / Última Atualização 10/04/2013 16:30 Agência Estado

Vigia dispara contra funcionário em banco de SP

Um vigia atirou contra seu supervisor em uma agência bancária na Avenida Paulista, em São Paulo

Um vigia atirou contra seu supervisor em uma agência bancária na Avenida Paulista, em São Paulo, por volta das 17h desta terça-feira (9). De acordo com a Polícia Militar, um desentendimento sobre uma causa trabalhista motivou o disparo. O funcionário baleado foi levado ao Hospital das Clínicas da capital, mas não resistiu e morreu.

Segundo a assessoria de imprensa do Banco Itaú, os dois envolvidos são funcionários de uma empresa de segurança terceirizada, a Vanguarda. O banco disse ainda que acompanha o caso e prestará todos os esclarecimentos necessários às autoridades.

Em nota, a Vanguarda lamentou o caso e disse que prestará total assistência aos familiares da vítima. Segundo a empresa, os dois funcionários trabalhavam na companhia desde 2006 e "sempre apresentaram comportamento profissional exemplar e nunca se envolveram em qualquer tipo de conflito". O motivo que desencadeou a discussão ainda será investigado.

O vigia foi preso e levado ao 78º Distrito Policial da cidade.

10/04/2013

02/06/2011

Vigilante atira em cliente de banco em Caxias

• O comerciante Felipe de Almeida Terra, de 32 anos, foi baleado no pescoço ontem, quando tentava entrar num banco em Duque de Caxias, na Baixada Fluminense. O tiro foi disparado pelo vigilante Alex Rosário Sandes após uma discussão provocada pelo travamento da porta giratória da agência. Preso em flagrante, o vigilante responderá por tentativa de homicídio.

Segundo a polícia, a confusão começou quando Felipe, que levava R$ 4 mil para depositar, foi impedido de entrar numa agência do Itaú devido ao travamento da porta. Um cliente se desentendeu com o comerciante e, do lado de fora do banco, os iniciaram uma briga, apartada pouco depois.

Após a confusão, Felipe deixou a bolsa e um celular com um amigo e foi reclamar do travamento da porta com o vigilante. Quando se aproximou, Alex disparou. Ele disse na 62ª DP (Imbariê) que agiu em legítima defesa. O delegado Hilton Alonso requisitou imagens do circuito interno da agência. ■

CAPA | PLANTÃO | MEU GLOBO | BLOGS | COLUNISTAS | EU-REPÓRTER

PAÍS | RIO | CIDADES | ECONOMIA | MUNDO | CIÊNCIA | ESPORTES | CULTUR

Publicada em **06/05/2010** às 20h21m Olá, Frederico

VIOLÊNCIA

Cliente com marcapasso é baleado por segurança de banco ao ser barrado em porta giratória SP

Cleide Carvalho, O Globo; SPTV; Jornal Nacional

DÊ SEU VOTO | MÉDIA: 4,3 | Comente

SÃO PAULO - Um homem de 47 anos, que usava marcapasso, foi baleado na cabeça por um segurança da agência do Bradesco em São Miguel Paulista, na Zona Leste de São Paulo. Um segundo cliente, um cozinheiro de 62 anos, também foi atingido de raspão pelo mesmo tiro.

Clique para ampliar

O crime ocorreu logo na abertura da agência, às 10h. Segundo testemunhas, todos aguardavam para entrar no banco.

Aposentado por problemas de saúde, Domingos Conceição dos Santos iria sacar o dinheiro da primeira aposentadoria. Foi barrado na porta giratória da agência por causa do marcapasso. Acabou discutindo com o segurança do banco, que disparou. O tiro atingiu a cabeça de Domingos, atravessou e feriu de raspão o nariz do cozinheiro.

Dois policiais militares que faziam a ronda a pé pela Rua José Otoni, onde fica a agência, foram avisados por rádio que havia ocorrido o disparo. Ao chegarem no local, viram o homem de 47 anos caído no chão, perto da porta giratória. Assustado, o cozinheiro saiu correndo, com o nariz sangrando.

O cliente baleado na cabeça foi levado em estado grave para o pronto socorro do Hospital Tide Setúbal, onde segue internado. O cozinheiro foi medicado e liberado em seguida.

O tiro teria sido disparado pelo segurança Pedro Gonçalves Almeida, de 37 anos. Ele foi preso em flagrante e autuado por dupla tentativa de homicídio doloso no 22º Distrito Policial de São Miguel Paulista. À polícia, o segurança disse que a vítima estava com comportamento alterado e achou que Domingos estivesse armado, e por isso atirou.

Em comunicado, o Bradesco diz que lamenta o ocorrido e está prestando assistência aos familiares das vítimas.

Resultados

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

25/65

Atividade

- Faça uma Análise de Riscos do seu Processo de Negócio

26/65

Análise CIDAL

- Agora que sei o que proteger, e do que proteger, COMO devo proteger ?
- Níveis diferentes de SENSIBILIDADE dentro de cada requisito permitem direcionar as ações

27/65

Quarto Passo: Avaliação da Sensibilidade

- Atributos da Informação (CIDAL)
  - Confidencialidade
  - Integridade
  - Disponibilidade
  - Autenticidade
  - Legalidade

28/65

Objetivos da Análise CIDAL

- Possibilitar a identificação de sensibilidade nem sempre óbvia
- Permitir soluções compatíveis com a natureza do risco
- Priorizar processos de acordo com suas sensibilidades ao risco

Caso

- Com a tabela de métricas fornecida, fazer o CIDAL para o Estudo de Caso
- As métricas devem ser construídas para atender os seguintes requisitos:
  - Foco na continuidade do negócio
  - Permitir uma comparação objetiva entre os processos, explorando a maior facilidade da avaliação qualitativa

Métricas para o Estudo de Caso

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 locais 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 globais 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

Resultados

Análise CIDAL com justificativas:

PN A	C	I	D	A	L
1			X		
2		X		X	
3	X				X
4					
5					

PN B	C	I	D	A	L
1					
2					X
3					
4	X			X	
5		X	X		

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.

Conclusão Objetiva: PN A: média 2,2 (relevante) e PN B: 4,0 (crítico)

Atividade

- Fazer uma tabela com possíveis efeitos impactantes compatíveis com o seu Processo de Negócio e fazer o CIDAL

Resultados até aqui

- Resultados
  - Documentação do PDS
  - Envolvimento de todos os Gestores
  - Início da formação da Mentalidade de Segurança
  - Melhor entendimento do negócio
  - Os diferentes índices de sensibilidade apontam para uma priorização de ações

Sensibilidade Temporal

- Ferramenta GUT
  - Usa os resultados da fase anterior
  - Agrega sensibilidade temporal em crise e na evolução do negócio
  - Permite maior priorização usando a multiplicação dos índices (no CIDAL é a média)

35/65

Objetivos do GUT

- Aprofundar o entendimento do ambiente
- Analisar tolerâncias temporais
- Inserir expectativas dos *stakeholders* no PDS
- Evoluir na priorização entre os Processos

36/65

Caso

- Usando a tabela abaixo, elaborar o GUT do Estudo de Caso

Tabela para o significado semântico dos índices:

	Gravidade (CIDAL)	Urgência	Tendência
1	Entre 1 - 2,3	Tolerância acima 120h	Não há menção no PN[1]
2	Entre 2,4 - 3,7	Tolerância entre 24 e 120h	Possibilidade de agravamento prevista no PN
3	Entre 3,8 - 5	Tolerância inferior 24h	Previsão de incremento previsto no PN

37/65

[1] Neste caso, PN significa *Plano de Negócios*

Resultado

Análise GUT

	Gravidade	Urgência	Tendência	Total
PN1	1	1	1	1
PN2	3	3	1	9

Prioridade entre os processos: PN2, mais prioritário que o PN1, o que significa que o PN2 é mais sensível, com maior nível de risco que o PN1.

38/65

Atividade

- Fazer o GUT do seu Processo de Negócio

Resultados até aqui

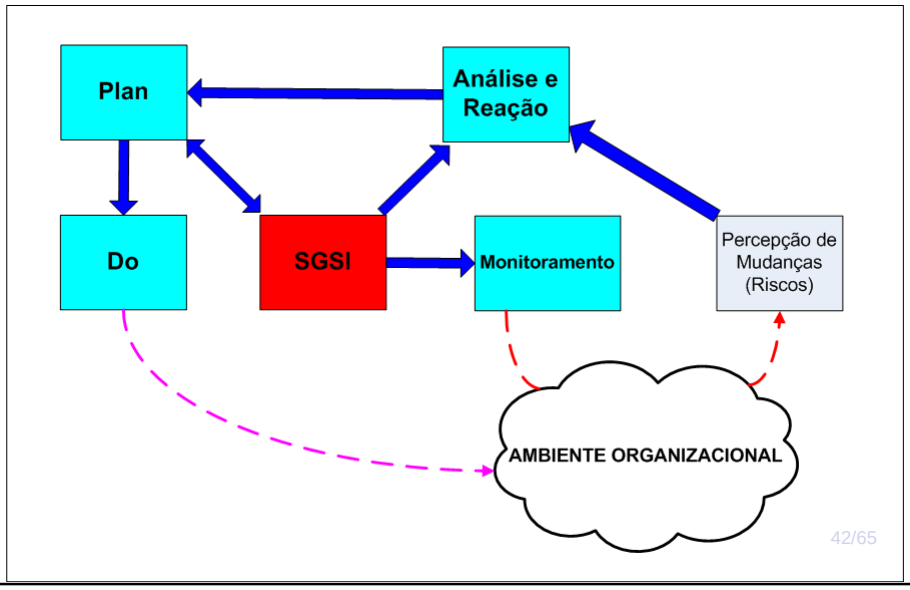
- Além do entendimento do negócio e da priorização entre os processos
  - Continuidade do processo de envolvimento dos Gestores
  - Continuidade da formação da Mentalidade de Segurança
  - Documentação do Plano Diretor de Segurança

Próximos Passos

- Encerra-se assim a fase de levantamento das características do negócio
- Próxima etapa (quinto passo): Montagem de uma Estrutura de Gestão do Risco
  - FSI ou CGSI ?
    - É importante ser *top-down* ?
    - É importante ser abrangente e democrática ?
    - É importante haver um *Security Officer* ?
  - Início do PDCA

41/65

PDCA Modificado

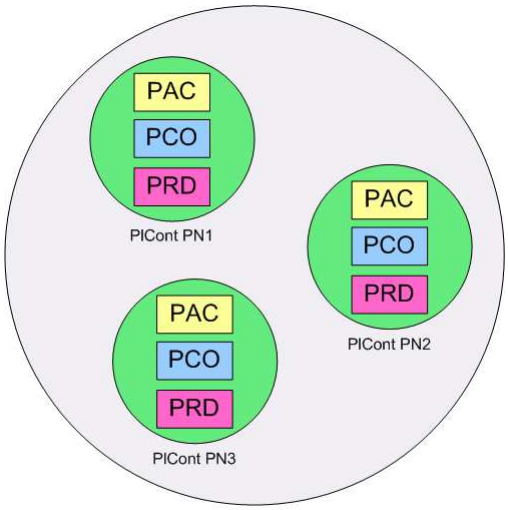


42/65

Sexto Passo

- Plano de Continuidade dos Negócios
  - Contém os “Planos B” para as situações de risco de alta criticidade
  - Devem ser criados para os PN, e não para os ativos – são os “Planos de Contingência”
  - Devem ser organizados para missões distintas:
    - PAC – Plano de Administração de Crise
    - PCO – Plano de Continuidade Operacional
    - PRD – Plano de Recuperação de Desastres

Plano de Continuidade dos Negócios (PCN)



PCN da Empresa

PCN

- O PCN deve ser único para toda a empresa
- É organizado em Planos de Contingência, elaborados por Processo de Negócio
- Modularizado em grupos de ações que podem ser executadas em paralelo, apesar disto não ser um requisito

45/65

Business Impact Analysis

- Ferramenta para priorização de processos de acordo com sua criticidade, tolerância temporal e impactos
- As ameaças mais relevantes devem ser evidenciadas para cada Processo de Negócio
- Assunto bem discutido na literatura, comum a cada tipo de negócio
- Maior dificuldade é a mensuração quantitativa dos impactos

46/65

Plano de Continuidade

- Elaborado para as necessidades mais impactantes (BIA)
  - Envolve questões orçamentárias
    - RoI – *Return of Investiment*
  - Deve, com o menor custo, garantir a funcionalidade do negócio dentro da tolerância temporal

47/65

Objetivo do PCN

- Além de buscar garantia de manutenção da funcionalidade dentro da tolerância desejada, visa evitar novas ocorrências
- Deve ser testado periodicamente (PDCA)

48/65

Caso

- Elaboração de um Plano de Contingência para a Pane Elétrica do PN 2 (ERP)

Resultado - PAC

Este Plano de Contingência, que junto com os demais comporá o Plano de continuidade dos negócios da empresa, deve ser organizado em três planos:

Plano de Administração da Crise (PAC) – Ao ocorrer uma pane elétrica, os recursos de controle entrarão em ação automaticamente. No entanto, por tratar-se de uma situação indesejada, que reduz a capacidade operacional da empresa, ações contingenciais são necessárias. No que diz respeito ao PAC, são ações cabíveis:

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;

Resultado - PCO

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;

51/65

Resultado - PRD

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.

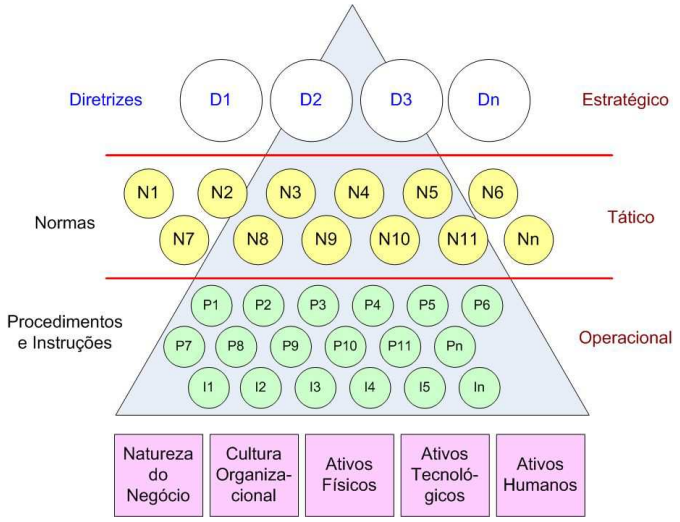
52/65

Sétimo Passo

- Política de Segurança (PolSeg)
  - É o dia-a-dia do controle do nível de risco
  - Depende de conscientização, treinamento e envolvimento *top-down*
  - Definida através de Diretrizes, Normas e Procedimentos
  - Deve focar objetivamente nos riscos evidenciados durante o mapeamento para o PDS
  - O Monitoramento demandará novas ações

53/65

PolSeg



54/65

Objetivos da PolSeg

- Os itens da PolSeg constituem dispositivos para controle do nível de risco
- Seus itens devem ser do domínio de todos os envolvidos em cada risco evidenciado
- Uma estratégia de capacitação deve garantir sua eficácia com eficiência

55/65

Caso

- Elaboração de ações de PolSeg focadas na Confidencialidade dos Dados (Diretriz), PN ERP (Norma) e Restrições de Acesso (Procedimentos)

56/65

Resultado

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:

a) Divulgação de produtos e serviços – apenas as quartas e sextas, das 14h às 15hs. mediante agendamento com o Gestor do PN:
b) 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
c) Visita de parentes de funcionários ao setor – vedadas.

57/65

Resultado (cont)

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.

58/65

Atividade

- Elabore um conjunto de Diretrizes, uma Norma e um Procedimento para controlar risco da ocorrência de incidentes de fraude no seu Processo de Negócio

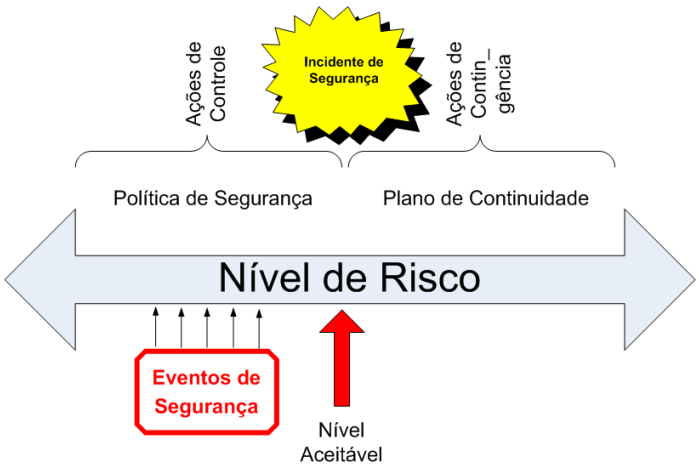
59/65

Próximo Passo

- Visando ativar o PDCA, o monitoramento contínuo e as auditorias permitem alterações nos PLCont e na PolSeg
- Uma Análise de Riscos agora pode ser feita com melhores resultados

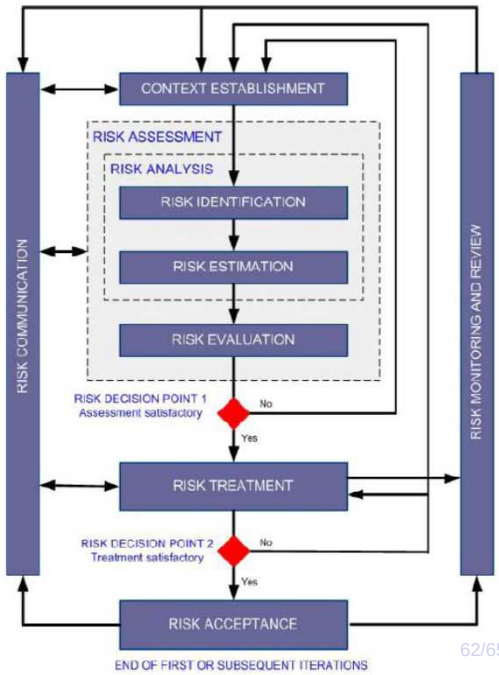
60/65

Desafio da Gestão do Risco



61/65

ISO 27005 Risk Management



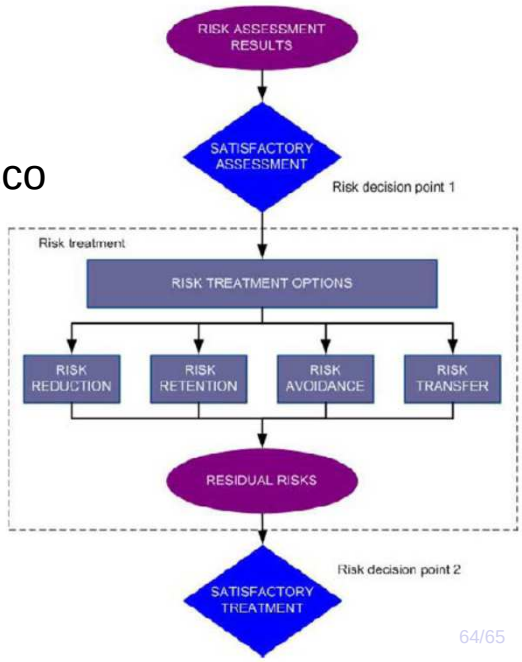
62/65

PDCA do Risco

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Risk treatment planning Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

63/65

Tratamento do Risco



64/65

Conclusão Final

- Segredo do Sucesso:
  - Comprometimento do setor executivo;
  - O uso de uma metodologia;
  - Envolvimento de todos os Gestores;
  - Criação de mentalidade de segurança, para alcançar o comprometimento dos colaboradores; e
  - Postura proativa, é possível manter o nível de risco sob controle.

65/65