Segurança de Redes

Gerenciamento e Avaliação de Riscos

Prof. João Henrique Kleinschmidt

Terminologia

- Risco
  - Possibilidade de sofrer perda ou dano; perigo
- Ataque
  - acesso a dados ou uso de recursos sem autorização
  - execução de comandos como outro usuário
  - violação de uma política de segurança, etc,
- Vulnerabilidade
  - É uma falha que pode permitir a condução de um ataque
- Incidente
  - A ocorrência de um ataque; exploração de vulnerabilidades
- Ameaça
  - Qualquer evento que pode causar dano a um sistema ou rede
  - A existência de uma vulnerabilidade implica em uma ameaça
- Exploit code
  - Um código preparado para explorar uma vulnerabilidade conhecida

Exemplos de Ameaças

- Pessoas chaves para uma organização
  - Ferimento, morte
- Servidores de arquivos
  - Ataques DoS
- Dados dos alunos
  - Acesso interno não autorizado
- Equipamentos de produção
  - Desastre natural

Exemplos de Vulnerabilidades

- Pessoas chaves para uma organização
  - Sem controle de acesso
- Servidores de arquivos
  - Aplicação incorreta de correções (patches)
- Dados dos alunos
  - Terceirizados não averiguados
- Equipamentos de produção
  - Controles fracos de acesso físicos

Gerenciamento de Riscos

- Estruturas de SI nas organizações são criadas para gerenciador riscos
- Gerenciar riscos é uma das responsabilidades dos gestores da organização
- Todos os programas de gerenciamento de riscos são baseados em dois processos
  - Identificação e avaliação de riscos
  - Controle (minimização) de riscos

Conhecimento do Ambiente

- Identificar, examinar e compreender
  - A informação e como ela é processada, armazenada e transmitida
- Iniciar um programa detalhado de gerenciamento de riscos
- O gerenciamento de riscos é um **processo**
  - Meios, salvaguardas e controles criados e implementados não devem ser "instale e esqueça"

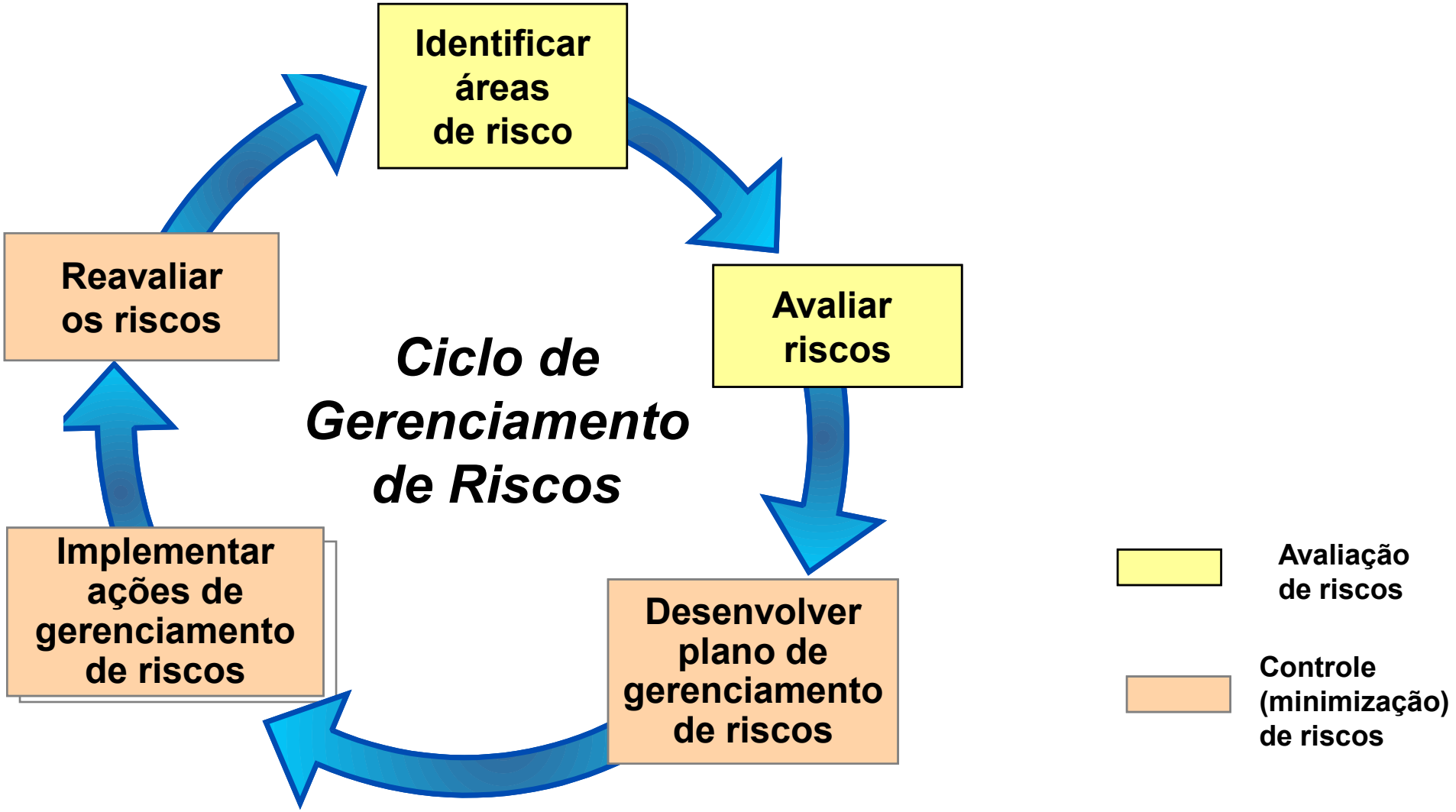
Conhecimento do inimigo

- Identificar, examinar e compreender
  - As ameaças
- Gestores devem estar preparados
  - Para identificar as ameaças que oferecem riscos para a organização e a segurança dos seus ativos
- O gerenciamento de riscos é um processo
  - De avaliar os riscos de uma informação e determinar como eles podem ser controlados (minimizados)

Gerenciamento de Riscos

- O processo de identificar, medir, controlar e minimizar os riscos de segurança a um nível proporcional ao valor dos ativos protegidos (NIST)
- Conjunto de atividades coordenadas para direcionar e controlar um organização com relação a riscos de SI (BS 7799-2)
- Processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável (ISO 17799)

Ciclo de vida Gerenciamento de Riscos



Definições ISO 27001

- Gerenciamento de riscos
  - Conjunto de atividades coordenadas para direcionar e controlar um organização com relação a riscos de SI
- Análise de riscos
  - Uso sistemático da informação para identificar as fontes de riscos e para estimar o risco
- Avaliação de riscos
  - Processo de comparar os riscos estimados com determinados critérios de riscos para determinar a significância dos riscos
- Estimativa de riscos
  - Processo global de análise e avaliação de riscos
- Tratamento de riscos
  - Processo de seleção e implementação de medidas para modificar o risco
- Aceitação de riscos
  - Decisão de aceitar um risco

ISO/IEC Guide 73

- Harmonização dos termos que compõem os documentos de especificação da segurança
- Deu fim à dificuldade no entendimento de termos como ameaças, vulnerabilidades, controles, probabilidade, impacto, consequências
- Gestão de riscos
  - Análise do Risco
  - Critérios de Risco
  - Avaliação do Risco
  - Tratamento do Risco
  - Comunicação do Risco

Norma ISO IS 13335

- Management of Information and Communication Technology (MICTS)
- Parte 1 – Conceitos e Modelos
- Parte 2 – Técnicas para Gerenciamento de Riscos da Informação e de Tecnologia de Comunicação

Padrão AS/NZS 4360

- Padrão da Austrália e Nova Zelândia para gerenciamento de riscos (genérico, não só de SI)
- Processo AS/NZS 4360
  - Estabelecer o contexto
  - Identificar os riscos
  - Analisar os riscos
  - Avaliar os riscos
  - Tratar os riscos
  - Monitorar e revisar
  - Comunicar e consultar

Gerenciamento de Riscos
Chave para o sucesso

- Compromisso da diretoria
- Suporte e participação da TI
- Competência da equipe de avaliação de riscos
- Consciência e cooperação dos usuários
- Avaliação contínua dos riscos críticos

Ferramentas para Avaliação de Riscos (AR)

- Avaliação de riscos pode ser feita manualmente, usando formulários, questionários e planilhas
- Em geral, em 80% dos casos, pode ser feita com o uso de planilhas bem projetadas
- Situações em que pode ser útil usar ferramentas
  - O volume de riscos é grande demais
  - Necessidade de que as alterações nos resultados da análise de riscos tenha controle de acesso rígido
  - O software se torna o cerne do processo de negócios, ou seja, existe uma integração profunda entre o processo de AR e a ferramenta que o suporta

Gerenciamento de Riscos
Guia do NIST Publicação NIST 800-30

Risk Management Guide for Information Technology Systems

Julho de 2002

Objetivo: A base para o desenvolvimento de um programa de gerenciamento de riscos efetivo, contendo as definições e orientação prática necessária para avaliar e minimizar os riscos identificados nos sistemas de TI

csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Procedimentos básicos

- Avaliação de Riscos – Quais são os riscos?
- Minimização de Riscos – O que fazer para tratar os riscos?
- Avaliação – Qual foi o resultado alcançado?

Estimativa de Riscos

- Passo 1: Caracterização do sistema
- Passo 2: Identificação das ameaças
- Passo 3: Identificação de vulnerabilidades
- Passo 4: Análise de controles
- Passo 5: Determinação das possibilidades
- Passo 6: Análise de impacto
- Passo 7: Determinação dos riscos
- Passo 8: Recomendações de controles
- Passo 9: Documentação

Estimativa de Riscos

- Passo 1: Caracterização do sistema
  - O que há para gerenciar?
  - Como a TI está integrada no processo?
- Passo 2: Identificação das ameaças
  - Quais fontes de ameaças devem ser consideradas?

    (Interna/externa, acidental/intencional, maliciosa/não-maliciosa)
- Passo 3: Identificação de vulnerabilidades
  - Quais falhas/fraquezas podem ser exploradas?
- Passo 4: Análise de controles
  - Quais são os controles atuais e planejados?

Estimativa de Riscos

Passo 5: Determinação das possibilidades

Alta	Fonte de ameaças altamente motivada e habilidosa e controles para prevenir exploração das vulnerabilidades são ineficazes
Média	Fonte de ameaças motivada e habilidosa, mas existem controles que podem impedir a exploração das vulnerabilidades
Baixa	Fonte de ameaças carente de motivação ou habilidade ou existem controles para prevenir a exploração das vulnerabilidades

Estimativa de Riscos

Passo 6: Análise de Impacto

A exploração da vulnerabilidade pode resultar em:

Alta	(1) perda de grandes ativos resultando em custo altíssimo; (2) violação, dano ou impedimento significativo da/na missão, reputação ou lucro; (3) morte ou ferimento humano
Média	(1) perda de ativos caros; (2) violação, dano ou impedimento da/na missão, reputação ou lucros; (3) ferimento humano
Baixa	(1) perda de algum ativo real; (2) influência visível na missão, reputação ou lucros

Estimativa de Riscos

Passo 7: Determinação dos riscos

Possibilidade da ameaça	Impacto		
	Baixo (10)	***Médio*** (50)	***Alto*** (100)
Alta (1.0)	***Baixo*** 10 X 1.0 = 10	***Médio*** 50 X 1.0 = 50	***Alto*** 100 X 1.0 = 100
Média (0.5)	***Baixo*** 10 X 0.5 = 5	***Médio*** 50 X 0.5 = 25	***Médio*** 100 X 0.5 = 50
Baixa (0.1)	***Baixo*** 10 X 0.1 = 1	***Baixo*** 50 X 0.1 = 5	***Baixo*** 100 X 0.1 = 10

Escala de Risco: Alto (>50 a 100); Médio (>10 a 50); Baixo (1 a 10)

Estimativa de Riscos

Passo 7: Determinação dos riscos

Nível do Risco	Descrição do Risco e Ações Necessárias
Alto	Se uma ameaça é avaliada como um risco alto, existe uma necessidade forte de medidas corretivas Um sistema existente pode continuar a operar, mas o plano de ação corretiva deve ser implantado **o mais rápido possível**
Médio	Se uma ameaça é avaliada como um risco médio, ações corretivas são necessárias e um plano deve ser desenvolvido para incorporar essas ações **em um tempo razoável**
Baixo	Se uma ameaça é avaliada como um risco baixo, a organização deve **determinar se ações corretivas são necessárias** ou decidir em aceitar o risco

Risk Assessment (Continued)

Passo 8: Recomendações de controles

- Objetivo: encontrar os controles mais baratos para garantir operação a pleno vapor
- Considerações:
  - Eficácia do controle
  - Legislação, regulamentação e política organizacional
  - Impacto operacional
  - Segurança física e confiabilidade

Os controles sempre devem ser adequados à organização

Minimização de Riscos

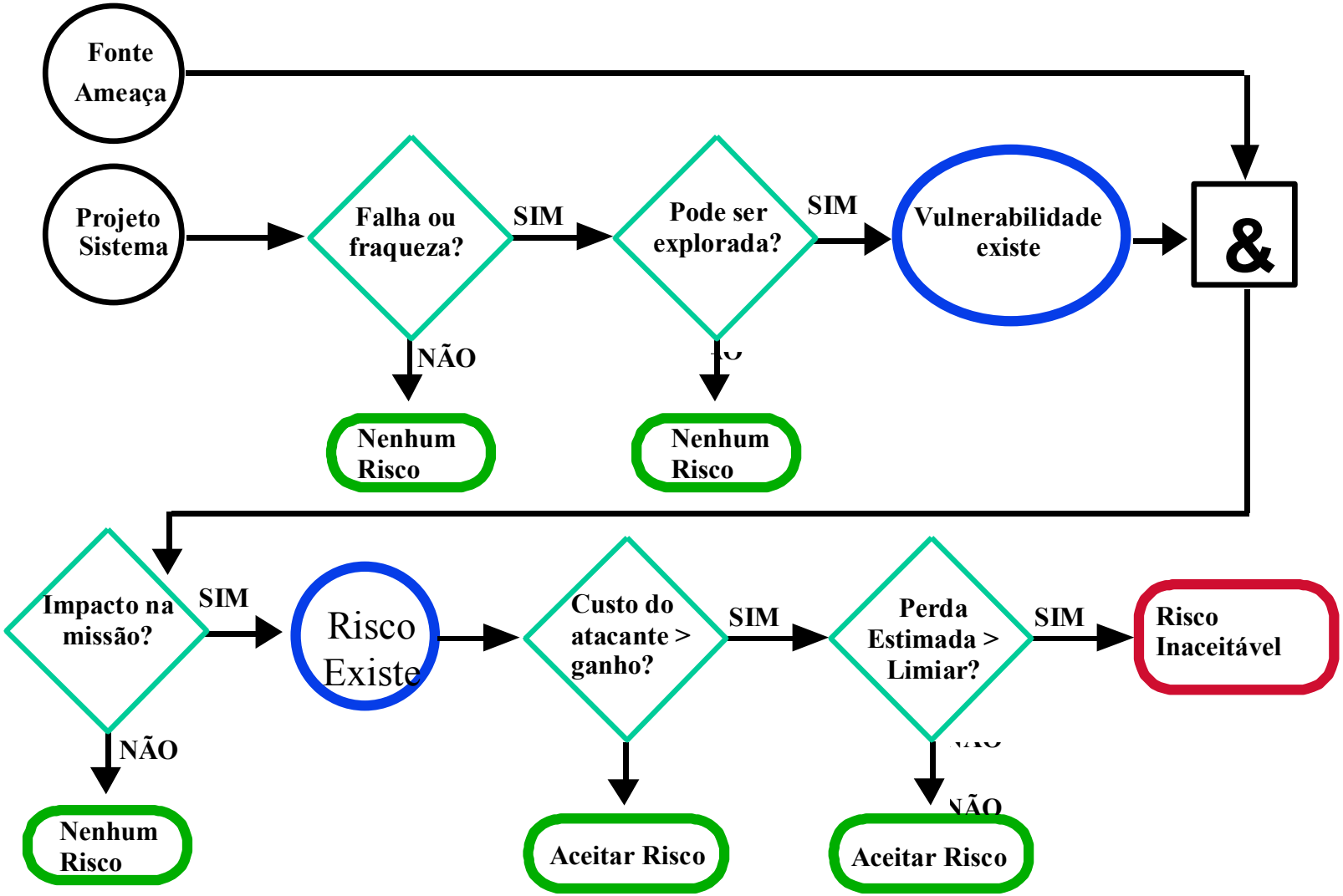
A diretoria e gerências devem assegurar que os controles mais apropriados são implementados para que a missão da empresa esteja sendo efetivamente sendo perseguida

Minimização de Riscos

Opções de minimização

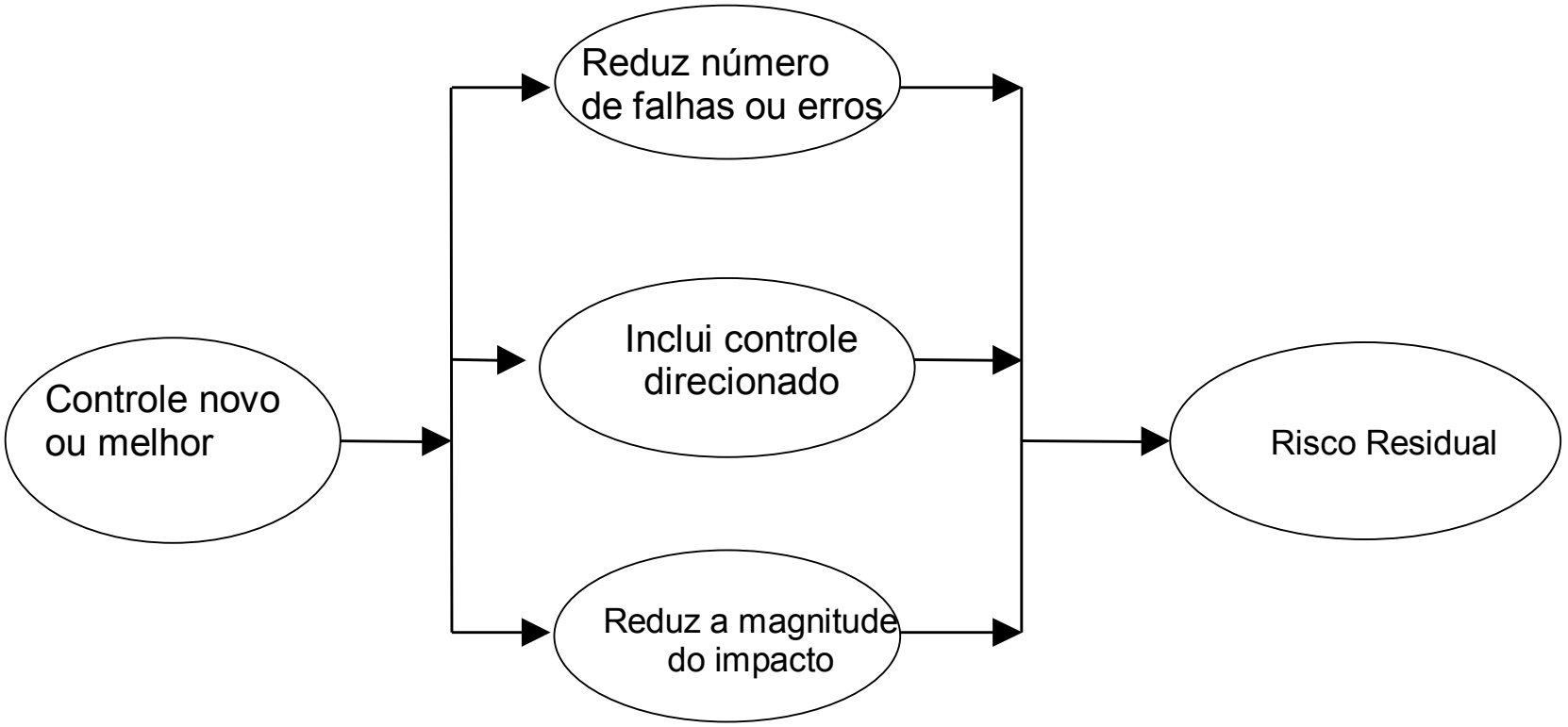
- Adoção/aceitação do Risco
  - Aceitar o risco potencial
- Anulação do Risco
  - Alteração da maneira como o sistema é utilizado
  - Remoção da vulnerabilidade ou possibilidade de exploração
- Limitação do Risco
  - Estabelecimento de limites no sistema, para detectar e reagir rapidamente
- Transferência do Risco
  - Para alguém que paga por ele (ex: seguro)

Estratégia para minimização de riscos



Minimização de Riscos
Implementação de Controles

- Técnico (Suporte, prevenção, detecção & recuperação)
- Gerencial (treinamento, planos, procedimentos)
- Operacional (físico, pessoal, backup, ...)

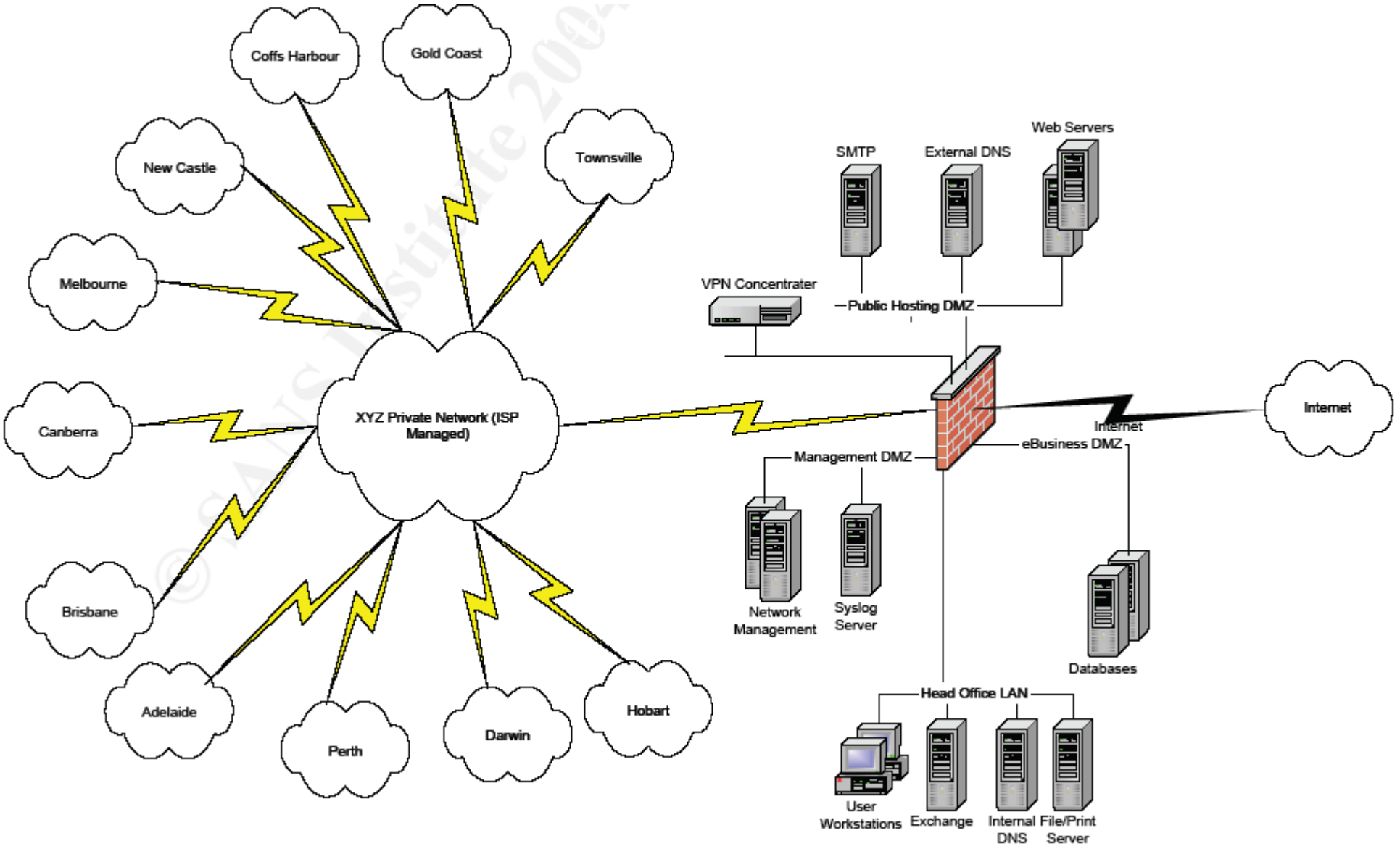


Exemplo de um ISMS para um "gateway" de acesso à Internet

Contexto do ISMS

- Associação XYZ: engenharia
- 12 locais conectados através de VPN
- Objetivo:
  - Fazer o ISMS para o "gateway" principal
- Projeto baseado na norma BS 7799-2
- Uso do modelo PDCA

ISMS para acesso à Internet



Redes que usam o gateway

- Internet
- E-Business
- LAN da Matriz
- Rede de Gerenciamento
- Rede privada da empresa (através do ISP)
- Rede de acesso remoto (VPN)
- Rede pública (DMZ): servidores web

Escopo do ISMS

- Acesso à Internet aos usuários internos
  - Web, email
- Serviços de hospedagem web
  - Servidores públicos
  - Serviços privados para os membros da associação
  - Hospedagem de páginas para os membros
- Acesso remoto para acesso via Internet (VPN)
- Infra-estrutura de TI
  - Firewall, servidores na DMZ, etc
- Segurança de informações dos sistemas que tiverem acesso via Internet
- Segurança física dos equipamentos
- Pessoal do departamento de TI

Situação atual da segurança

- Bom projeto técnico da segurança do gateway
- Manutenção e operação dos equipamentos e software executados de forma ad-hoc
- Não existem procedimentos e planos para a operação dos equipamentos
- Praticamente sem política(s) de segurança
- Existem duas políticas de uso aceitável
  - Navegação da web
  - Uso de e-mail

ISMS: Fase "Plan"

- Metodologia para desenvolvimento do ISMS
  - Passos a serem executados
- Avaliação de riscos
  - Conduz o processo de desenvolvimento do ISMS
  - As atividades seguintes dependem da avaliação
- Desenvolvimento de uma estrutura de gerenciamento do ISMS
- Definição de uma política de segurança para o gateway da associação XYZ

ISMS: Fase "Plan"
Passos para o desenvolvimento

- Passo 1: Plano do projeto
- Passo 2: Avaliação (estimativa) de riscos
- Passo 3: Estrutura de gerenciamento do ISMS
  - Baseada na avaliação de riscos
- Passo 4: Política de segurança
  - Baseados na avaliação de riscos
  - Inclui diretrizes e procedimentos

ISMS: Fase "Plan" Passo 1: Plano do projeto

- O processo de desenvolvimento do ISMS necessita do envolvimento de todos os grupos interessados
  - Clientes, acionistas, fornecedores, funcionários
- Componentes do plano
  - Work Breakdown Structure (WBS)
    - Lista de tarefas e sub-tarefas (as vezes em forma de árvore)
  - Identificação dos envolvidos (stakeholders)
  - Início e fim das tarefas do WBS
  - Riscos do projeto
  - Aprovação do plano de projeto pela diretoria da XYZ

ISMS: Fase "Plan"
Passo 2: Avaliação de riscos

- Uso da metodologia AS/NZS 4360
  - Estabelecer o contexto
  - Identificar riscos
  - Analisar riscos
  - Avaliar riscos
  - Tratar riscos

ISMS: Fase "Plan"
Passo 2: AS 4360: Identificar

- Identificação das ameaças e vulnerabilidades que podem causar um incidente de segurança
- Natureza e fonte do risco
  - O que pode acontecer ou dar errado?
  - Como pode acontecer?
  - Por que pode acontecer?
  - Quem ou o que pode ser machucado/danificado
- O resultado *é* o **registro de riscos**

ISMS: Fase "Plan"
Passo 2: AS 4360: Identificar

- Serviço de Internet: **disponibilidade**
  - Dispositivos críticos de rede (roteador, firewall)
- Serviço de Internet: **disponibilidade**
  - Ataque DoS vindo da Internet
- Informações: **integridade**
  - Ataque de hackers da Internet
- Informações: **confidencialidade**
  - Ataque de hackers da Internet
- Infra-estrutura do gateway: **integridade**
  - Configuração errada acidental de um dispositivo de imposição de segurança

ISMS: Fase "Plan"
Passo 2: AS 4360: Analisar

- Critérios de possibilidade de ocorrência

Level	Description
Negligible	Unlikely to occur.
Very Low	Likely to occur two/three times every five years
Low	Likely to occur once every year or less
Medium	Likely to occur once every six months or less
High	Likely to occur once every month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times per day

ISMS: Fase "Plan"
Passo 2: AS 4360: Analisar

- Critérios de conseqüência

Level	Description
Insignificant	Will have almost no impact if threat is realised
Minor	Will have some minor effect on the asset value. Will not require any extra effort to repair or reconfigure gateway.
Significant	Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals. May result in compromise of limited amount of hosted data. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of the association, and/or notable loss of confidence in the gateway resources or services. Will require expenditure of significant resources to repair.
Serious	May cause extended gateway outage, and/or loss of business confidence by partners/members. May result in compromise of large amounts of hosted data.
Grave	Compromise of Association's sensitive data in the internal network causing permanent damage to Association's reputation. May cause permanent closure of Association's eBusiness initiative.

ISMS: Fase "Plan"
Passo 2: AS 4360: Analisar

- Critérios de avaliação

Consequence

Threat Likelihood	Insignificant	Minor	Significant	Damaging	Serious	Grave
Negligible	Nil	Nil	Nil	Nil	Nil	Nil
Very Low	Nil	Low	Low	Low	Medium	Medium
Low	Nil	Low	Medium	Medium	High	High
Medium	Nil	Low	Medium	High	High	Critical
High	Nil	Medium	High	High	Critical	Extreme
Very High	Nil	Medium	High	Critical	Extreme	Extreme
Extreme	Nil	Medium	High	Critical	Extreme	Extreme

ISMS: Fase "Plan"
Passo 2: AS 4360: Avaliar

- Riscos podem variar de "Nil" até "Extreme"
- Devem ser comparados com os níveis de "riscos aceitáveis" da fase "estabelecer contexto"
- Tabela de classificação de riscos

Level	Numerical Value
Nil	0
Low	1
Medium	2
High	3
Critical	4
Extreme	5

ISMS: Fase "Plan"
Passo 2: Registro de risco

Risk ID	Asset Identification	Threat to the Asset	Threat Likelihood Estimate	Consequence, if the threat is realised	Resultant Risk Level	Required Threat Likelihood	Required Consequence, if threat is realised	Required Risk	Countermeasure(s) Priority	Countermeasure(s) Recommendation based on AS/NZS 7799.2
1	XYZ Association's Internet services -- Availability	Critical network device (e.g. router, firewall, etc.) failure	Low	Significant	Medium	Very Low	Significant	Low	1	A.7.2.1 Equipment siting and protection A.7.2.2 Power supplies A.7.2.4 Equipment maintenance A.8.1.3 Incident management procedures A.8.2.1 Capacity planning A.8.2.2 System acceptance A.8.5.1 Network controls A.11.1.1 Business continuity management process A.11.1.2 Business continuity and impact analysis A.11.1.3 Writing and implementing continuity plans A.11.1.4 Business continuity planning framework A.11.1.5 Testing, maintaining and re-assessing business continuity plans
2	XYZ Association's Internet services -- Availability	Denial of Service attack from Internet	Very High	Significant	High	Very Low	Minor	Low	2	A.6.3.1 Reporting security incidents A.6.3.2 Reporting security weaknesses A.6.3.3 Reporting software malfunctions A.6.3.4 Learning from incidents A.8.1.3 Incident management procedures A.8.3.1 Controls against malicious software A.8.5.1 Network controls A.9.7.1 Event logging A.9.7.2 Monitoring system use A.9.7.3 Clock synchronization A.11.1.1 Business continuity management process A.11.1.2 Business continuity and impact analysis A.11.1.3 Writing and implementing continuity plans A.11.1.4 Business continuity planning framework A.11.1.5 Testing, maintaining and re-assessing business continuity plans
3	XYZ Association's Data - Integrity	Compromised network security by hackers from the Internet	Low	Serious	High	Negligible	Damaging	Nil	3	A.6.3.1 Reporting security incidents A.6.3.2 Reporting security weaknesses A.6.3.3 Reporting software malfunctions A.6.3.4 Learning from incidents A.8.1.3 Incident management procedures A.8.3.1 Controls against malicious software A.8.5.1 Network controls A.9.7.1 Event logging A.9.7.2 Monitoring system use

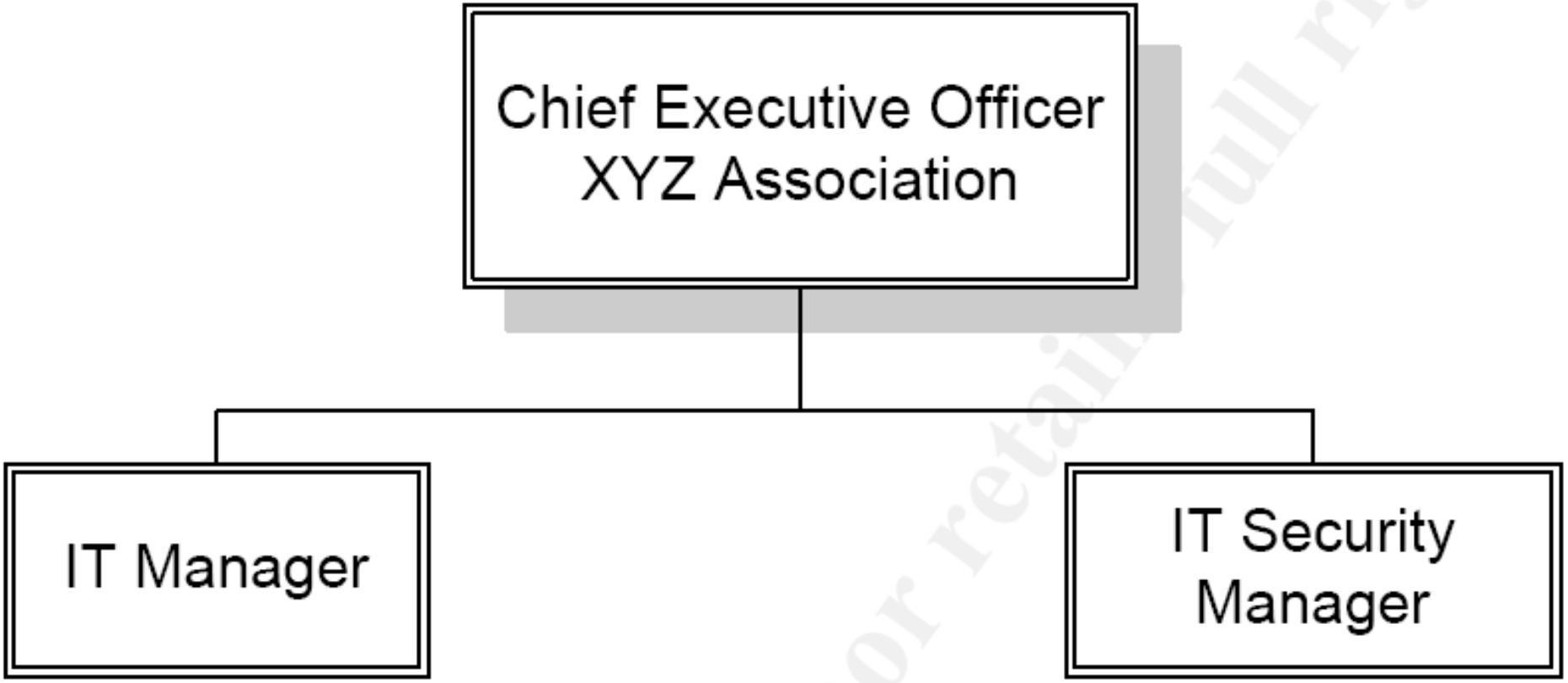
ISMS: Fase "Plan"
Passo 3: estrutura gerencial

- A definição de uma estrutura gerencial deve ser uma consequência da avaliação de riscos
- Objetivos
  - Demonstrar o compromisso da diretoria com o ISMS
  - Demonstrar que a estrutura gerencial faz cumprir o princípio de separação de responsabilidades nas operação do "gateway"

ISMS: Fase "Plan" Passo 4: políticas

- Áreas de políticas cobertas pelo ISMS
  - Política de acesso ao gateway
  - Política de segurança física
  - Política relativa às pessoas
  - Política de acesso a sistemas
  - Política de controle de configuração
  - Política de gerenciamento de mudanças
  - Política de detecção e resposta a incidentes
  - Política de contingência
  - Política de uso aceitável

ISMS: Fase "Plan"
Estrutura gerencial do ISMS



ISMS: Fase "Plan"
Políticas de segurança

2.4.1 Gateway access policy

Purpose: The purpose of the policy is to ensure that uncontrolled access to the XYZ Association internal network and the DMZs from the Internet is prevented. It also ensures that only controlled access from the association's internal network to the Internet and DMZs is permitted. This policy should detail at a high level the type of service (protocol) permitted by the gateway.

Intended Audience: The policy is intended for the staff managing the gateway. Certain relevant extracts from this policy should be included in the general staff awareness program.

Areas of the standard (AS/NZS 7799.2) covered: This policy covers the following areas of the standard:

- A.9.1.1 Access control policy
- A.9.4.1 Policy on use of network Services

ISMS: Fase "Do"

- Baseado nos requisitos da fase "Plan", essa fase implementa os controles selecionados
- Uso da técnica de Análise de Insuficiência
  - "gap analysis"
- Cada insuficiência (gap) é mapeada como um problema, porque se distancia do planejado
- São apresentadas para cada problema:
  - Ação: para remediar o problema
  - Passos: para implementar a ação

ISMS: Fase "Do"
Problema: IDS inexistente

- A avaliação e riscos detectou a necessidade de um controle para monitorar intrusões de rede
- Ação
  - Projetar uma solução de NIDS e desenvolver e implementar processos para fazer o monitoramento
- Passos
  - Definir NIDS (desenvolver, sw livre, comercial)
  - Comprar equipamentos
  - Instalar NIDS
  - Treinar equipe de monitoramento
  - Incluir saídas do NIDS no plano de detecção e resposta a incidentes de segurança

ISMS: Fase "Check"

- Uma lista de verificação deve ser feita para as atividades de verificar e auditar
- Para cada verificação, o objetivo de controle da contra-medida que está sendo auditada é discutido
- Lista de verificação
  - Descrição da verificação
  - Objetivo de controle
  - Razão para auditar
  - Passos para auditar
  - Frequência

ISMS: Fase "Check"
Lista de verificação

No	Audit Description	Control Objective (as per AS/NZS 7799.2:2003)	Reason for Audit	Steps for Audit	Frequency
4	Operational Procedures audit – change management plan, incident management plan	(A.8.1) To ensure the correct and secure operation of information processing facilities.	It is important for the Internet Gateway to have documented operational procedures. It is even more important to make sure that those procedures are followed.	1. Acquire change control records. Verify they are recorded as per plan. 2. Acquire incident response records and verify they are filled up as per plan.	Bi-annual
5	Anti virus application log and signature file audit	(A.8.3) To protect the integrity of software and information from damage by malicious software.	The threat of malicious software is real. It is very relevant to the gateway operations. There are virus scanning solutions implemented to detect malicious code. It is important to verify that they are working properly and when an event of malicious software is detected, it does not go unnoticed.	1. Execute command to check the virus signature version. 2. Verify that the version is up to date. 3. Access virus scanner logs and verify detected viruses are cleaned or appropriately quarantined and alert sent to monitors.	Daily
6	Backup and Restore audit	(A.8.4) To maintain the integrity and availability of information processing and communication services.	Backup system is integral to secure operation of the Internet Gateway. It is important and necessary that backup system operates regularly and backed up media is usable.	1. Access backup system logs and verify that backup takes place regularly and successfully. 2. Verify backup tapes are labelled properly by random checking. 3. Verify tapes are usable by executing a restore function	Bi-annual

ISMS: Fase "Act"

- Aprimoramento e manutenção do ISMS
- A auditoria verifica a não conformidade do planejado para o praticado com o ISMS
- Quando uma não conformidade é detectada, medidas corretivas e/ou preventivas devem ser tomadas, resultando em um ISMS aprimorado
- O objetivo é eliminar as não conformidades

ISMS: Fase "Act"

No	Audit Description	Possible Nonconformity	Possible Corrective / Preventive action
1	"Inventory of Assets" audit.	Inventory list is incomplete or erroneous.	a. Correct the list. b. Train staff to ensure inventory control procedure is followed.
2	Personnel security audit	Insufficient evidence of staff screening.	a. Complete staff screening. b. Train staff to ensure screening process is followed while recruiting.
		"Confidentiality Agreement" not signed.	a. Sign "Confidentiality Agreement". b. Ensure the process is followed properly in future.
		Security Brief not completed.	a. Complete the security brief. b. Ensure the process is followed in future.
3	Physical security audit	Inconsistent visitor logs.	Train the staff on access process.
		Inconsistent rack access logs.	Train the staff on rack access process.
		Anomalies in EACS logs.	Investigate and decide corrective or preventive action.