SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

SEGURANÇA DA INFORMAÇÃO

E NORMAS APLICÁVEIS

LUIS AMORIM

26 Mar 2022

2 SÍNTESE

- Introdução à ISO 27001
- Introdução à Gestão de Risco

3 EXEMPLIFICAÇÃO

- Ameaça: Inundação

(http://www.youtube.com/watch?v=ttcQy3bCiiU)

4 EXEMPLIFICAÇÃO

- Ameaça: Social Engeneering

(https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402)

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

PRO CYBER NEWS

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

PHOTO: SIMON DAWSON/BLOOMBERG NEWS

By Catherine Stupp
Updated Aug. 30, 2019 12:52 pm ET

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company's insurance firm, Euler Hermes Group SA.

5 EXEMPLIFICAÇÃO

- Ameaça: Social Engeneering

(https://www.reuters.com/article/us-facc-cyber-arrest-china-idUSKCN1110PR)

AEROSPACE AND DEFENSE AUGUST 26, 2016 / 9:16 AM / UPDATED 6 YEARS AGO

Chinese man arrested in Hong Kong over FACC cyber attack in Austria

By Reuters Staff 3 MIN READ

VIENNA (Reuters) - A Chinese citizen has been arrested in Hong Kong in connection with a cyber attack that cost Austrian aerospace parts maker FACC 42 million euros ($47.39 million), Austrian police said on Friday.

FACC fired its chief executive and chief financial officer after the attack, which involved hoax emails asking an employee to transfer money for a fake acquisition project - a kind of scam known as a “fake president incident”. FACC’s customers include Airbus and Boeing.

A 32-year-old man, who was an authorized signatory of a Hong Kong-based firm that received around 4 million euros from FACC, was arrested on July 1 on suspicion of money laundering, a spokesman for Austria’s Federal Office for Crime said.
Such attacks, also known as “business email compromise”, involve thieves gaining access to legitimate email accounts inside a company – often those of top executives – to carry out unauthorized transfers of funds.
The technique, which relies on simple trickery or more sophisticated computer intrusions, typically targets businesses working with international suppliers that regularly perform wire transfers.
A spokesman for FACC said the company was working on getting back 10 million euros which had been found and frozen on accounts in different countries around the world. These 10 million euros are not included in the 42 million euro hit the group has already booked.

In June, the U.S. Federal Bureau of Investigation (FBI) said identified losses from this scam totaled $3.1 billion and had risen by 1,300 percent in the past 18 months.

6 EXEMPLIFICAÇÃO

- Ameaça: Phishing

(https://www.wsj.com/articles/beware-of-qr-code-scams-11647625020?page=1)

JOURNAL REPORTS: TECHNOLOGY

Beware of QR Code Scams

It's so easy to click on a QR code. Criminals are counting on it.

By Heidi Mitchell
Updated March 19, 2022 8:00 am ET

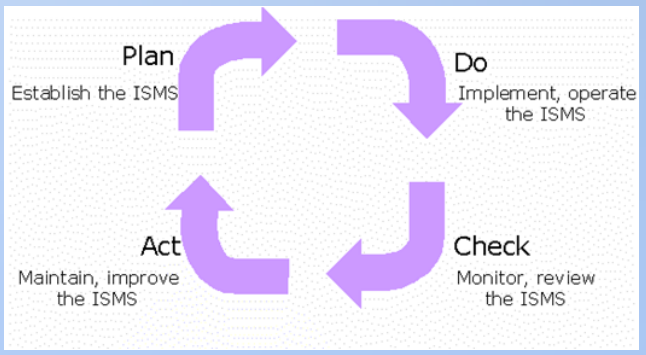
During the Super Bowl in February, one ad grabbed a lot of attention: a mysterious bouncing QR code that enticed viewers to point their phones at their screens and click through to an unknown website. (Spoiler alert: It was for Coinbase. COIN -1.83% ▼) Within seconds, more than 20 million people had done just that, crashing the cryptocurrency-exchange platform.

The incident illustrated just how willing people are to click on QR codes, but unfortunately for consumers, marketers aren't the only group that understands this. Two months before, in December, a much darker scenario involving QR codes unfolded when malicious actors placed QR-code stickers on parking meters in major Texas cities, directing drivers to a fraudulent website where they supposedly could pay for parking.

"People were tricked into putting in their credit-card information," says Eric Chien, security threat researcher at Symantec, part of Broadcom Software's security technology and response division. "It was a really well-done attack."

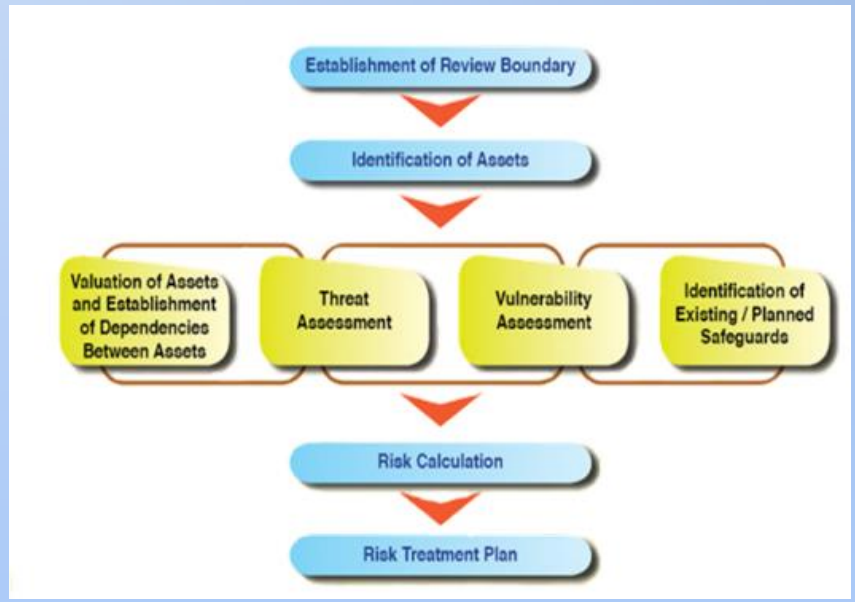
7 SÍNTESE

- Introdução à ISO 27001
  - ISO/IEC 27001- Information Security Management Systems
    - "specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks.
    - It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof."
  - O modelo PDCA para o ISMS
  - A versão atual ISO/IEC 27001:2013
- Introdução à Gestão de Risco



8 SÍNTESE

- Introdução à ISO 27001
- Introdução à Gestão de Risco
  - Risco é a probabilidade de algo mau vir a acontecer e causar danos a um ativo de informação
  - Existem várias formas de calcular o risco, em função da metodologia adotada e do tipo de organização
  - Após cada avaliação dos Riscos, estes devem ser tratados de acordo com o seu valor e as prioridades para o negócio
  - O standard a seguir é a ISO 27005 ou a ISO 31000



9 EXERCÍCIO DE GRUPO

- Escolher uma área/sistema da Universidade
- Identificar possíveis
  - Ameaças
  - Vulnerabilidades
  - Riscos
- Identificar controlos a implementar

10 AGENDA

- **Introdução à Gestão de Continuidade de Negócio**
- A avaliação e gestão de riscos
- Tratamento dos Riscos
- Controlos de segurança
  - Tecnológicos, Operacionais e de Gestão

INTRODUÇÃO À GESTÃO DE CONTINUIDADE DE NEGÓCIO

- A caracterização e implementação de um Business Continuity Management (BCM), ou Gestão Continuidade de Negócio deve fazer parte da Gestão de Risco de uma organização.
- O processo de Gestão Continuidade de Negócio conduz à produção de planos e procedimentos que permitem, a uma organização, responder a incidentes mantendo ou reactivando em tempo útil os seus serviços críticos ou essenciais para o negócio
- A dependência das organizações face aos Sistemas de Informação e os riscos a que se expõem torna necessário conceber e operacionalizar uma eficaz e eficiente Gestão Continuidade de Negócios.
- Actualmente o standard a seguir nesta área é a ISO 22301:2019
  - Revisão da versão 2012 (ainda utilizada)
  - Provém da BS25999 do BSI

12 INTRODUÇÃO À GESTÃO DE CONTINUIDADE DE NEGÓCIO

- Business Continuity Management Lifecycle (ISO 22301)

- BCM program management
- Understanding the organization
- Determining BCM strategies
- Developing & implementing a BCM response
- Exercising, maintaining and reviewing BCM
- Embedding BCM in the organization's culture

13 INTRODUÇÃO À GESTÃO DE CONTINUIDADE DE NEGÓCIO

- Uma Gestão de Continuidade de Negócio eficiente permite à Organização:
  - Identificar os processos/informação/sistemas críticos para o negócio
  - Identificar os impactos de uma eventual descontinuação dos serviços;
  - Preparar a resposta a incidentes, que permitam minimizar esses impactos para o negócio;
  - Definir processos e organização da equipa na sua implementação, testes e ativação;

- Oferece à organização uma vantagem competitiva
  - Em caso de incidentes, oferecendo uma maior preparação e rápida resposta
  - Pode ser explorado em termos de marketing

14 INTRODUÇÃO À GESTÃO DE CONTINUIDADE DE NEGÓCIO

- Uma Gestão de Continuidade de Negócio eficiente permite à Organização:
  - Identificar os processos/informação/sistemas críticos para o negócio
  - Identificar os impactos de uma eventual descontinuação dos serviços;
  - Preparar a resposta a incidentes, que permitam minimizar esses impactos para o negócio;
  - Definir processos e organização da equipa na sua implementação, testes e ativação;

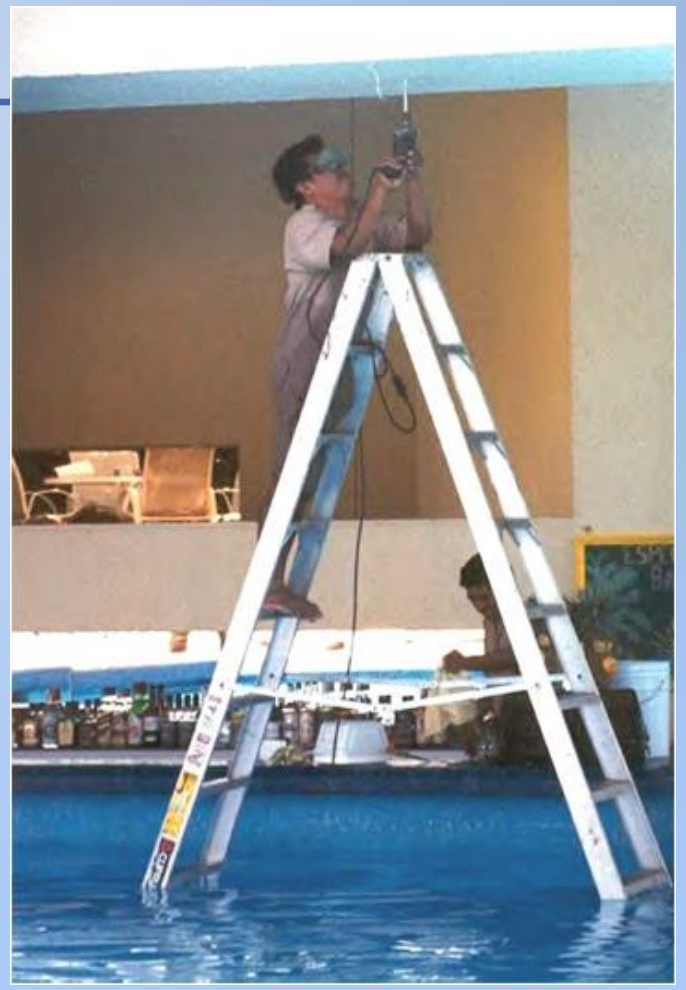
- Oferece à organização uma vantagem competitiva
  - Em caso de incidentes, oferecendo uma maior preparação e rápida resposta
  - Pode ser explorado em termos de marketing

15 AGENDA

- Introdução à Gestão de Continuidade de Negócio
- **A avaliação e gestão de riscos**
- Tratamento dos Riscos
- Controlos de segurança
  - Tecnológicos, Operacionais e de Gestão

16 A AVALIAÇÃO E GESTÃO DOS RISCOS

- ~~Análise de Risco?~~
- ~~Gestão do Risco?~~

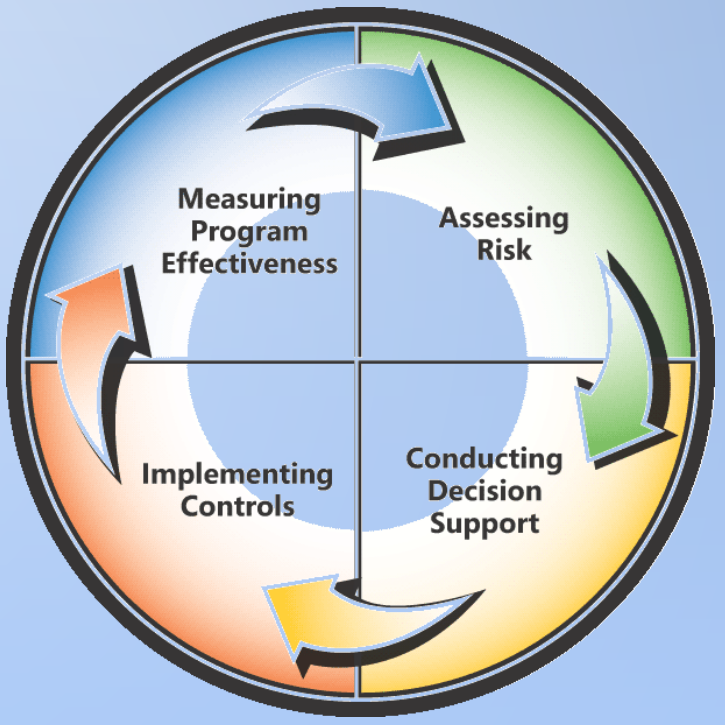


17 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Avaliação de Risco

  Vs

- Gestão de Risco
  - É um processo:
    - Avaliação de Risco
    - Decisões sobre opções
    - Implementação de controlos
    - Reavaliação/monitorização

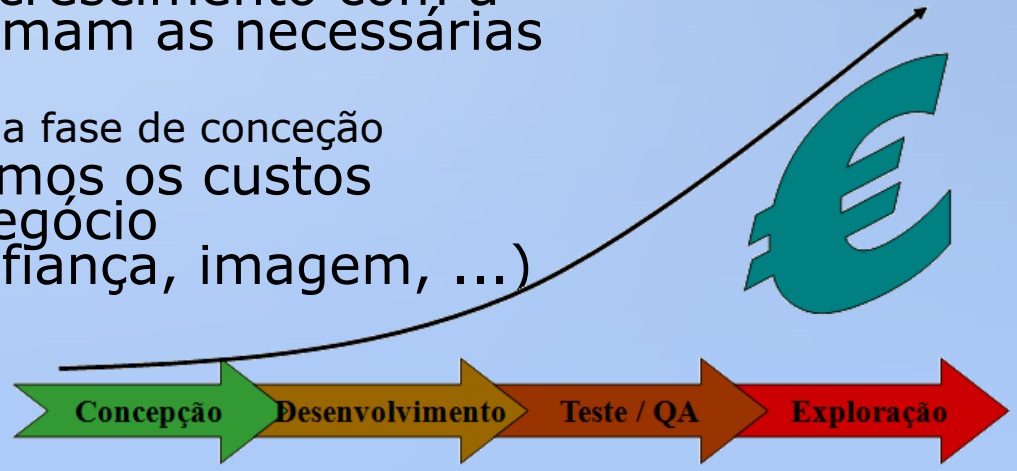


18 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Gestão de Riscos
  - Tem como objetivo permitir à organização atingir os objetivos a que se propôs:
  - Mantendo em segurança os sistemas de informação que guardam, processam ou transmitem informação da organização
  - Permitindo à gestão a tomada de decisões devidamente fundamentadas que justifiquem os investimentos e custos das Tis
  - Assistir a gestão na acreditação dos sistemas de IT com base na documentação resultante das atividades desenvolvidas na Gestão de Risco
  - É um processo, não um projeto

19 A AVALIAÇÃO E GESTÃO DOS RISCOS

- A aplicação da Avaliação e Análise de Risco:
  - Sobre os processos e sistemas implementados
  - Sobre novos processos e sistemas
- Ter em atenção que
  - O custo para correção de problemas de um sistema de informação apresenta um acentuado crescimento com a fase de vida do projeto, em que se tomam as necessárias medidas.
    - O ideal é ser realizada uma análise cuidada na fase de conceção
  - A acrescer aos custos de correção, temos os custos inerentes às consequências para o negócio (produtividade, indisponibilidade, confiança, imagem, ...)

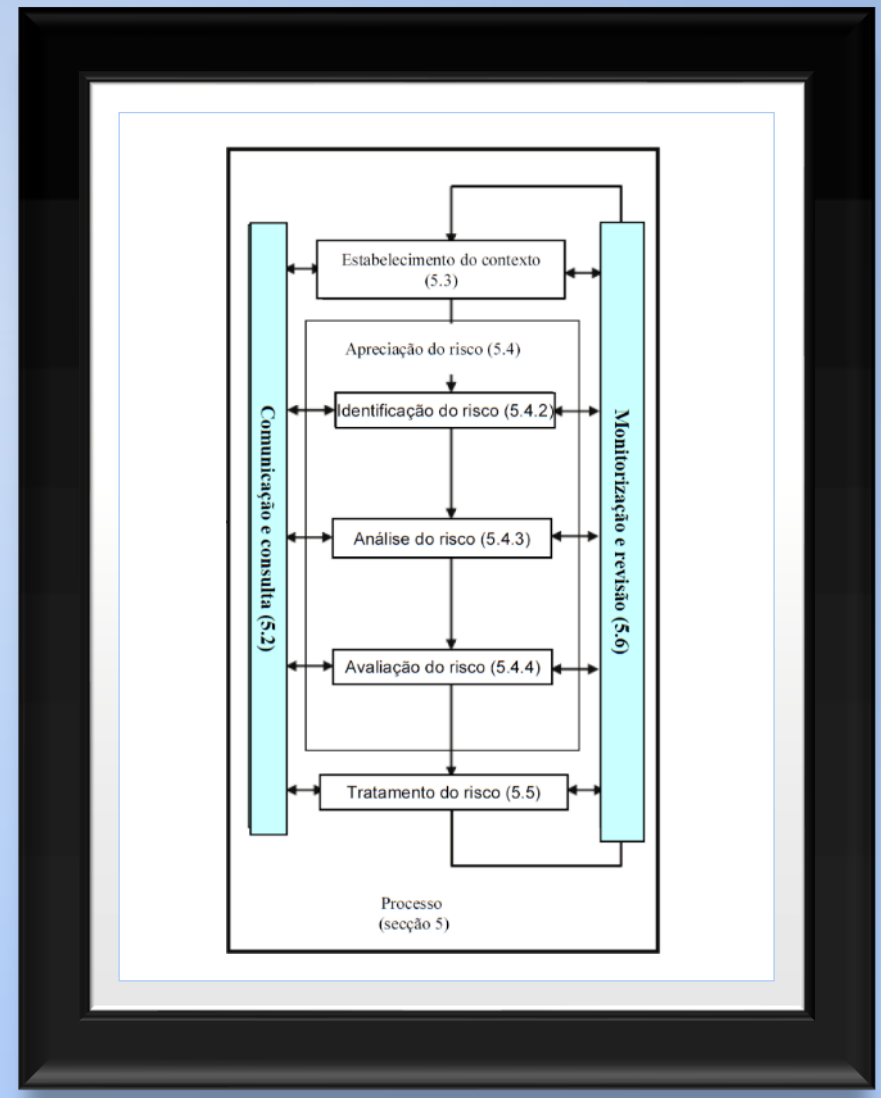


20 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Conceito em termos de Project Impact Analysis
  - Project Impact Analysis ou Avaliação dos Riscos de Projeto
    - É utilizada para fundamentar as razões pelas quais o processo deve ser (ou não) implementado
  - Avaliação de Risco do projeto
    - Depois de analisado e aprovado, a avaliação serve para identificar as ameaças inerentes a esse projeto, e possível redução de riscos
  - Resultados principais
    - Identificação das ameaças e Valorização dos Riscos
    - Identificação de possível formas de mitigação
    - Análise custo benefício da implementação

A AVALIAÇÃO E GESTÃO DOS RISCOS

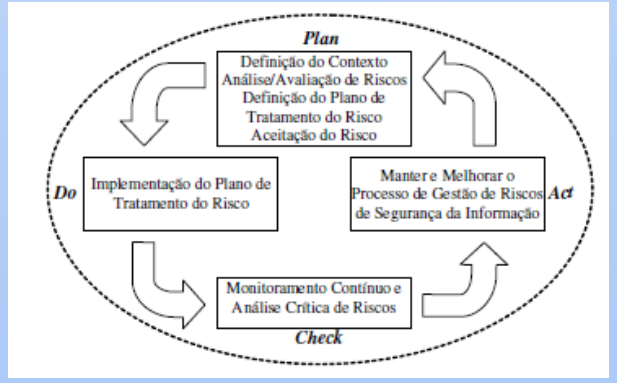
- ISO 31000:2009 - Risk management - Principles and guidelines
- Norma ISO genérica que define metodologia de Gestão de Risco

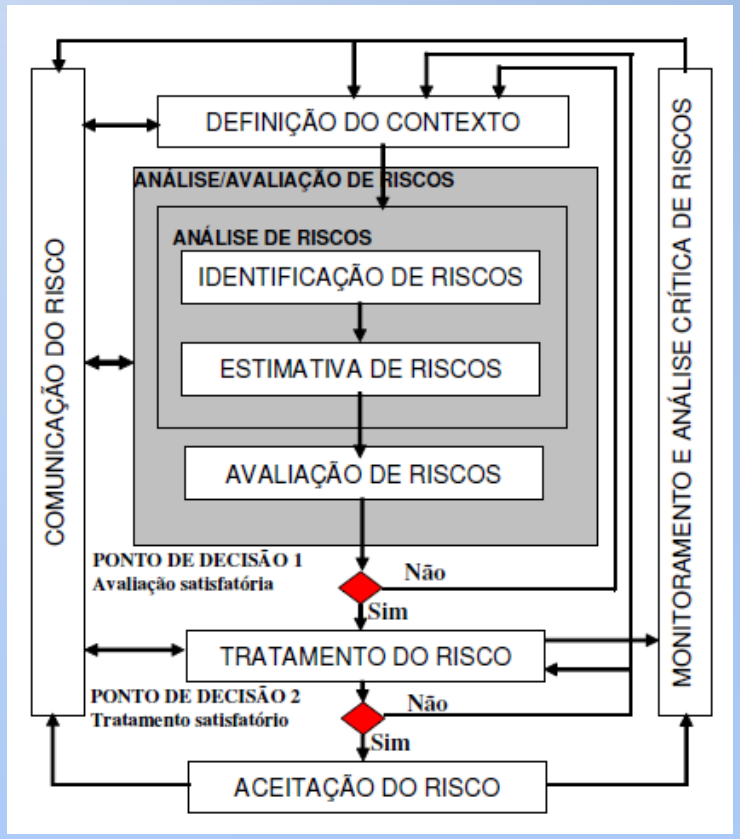


22 A AVALIAÇÃO E GESTÃO DOS RISCOS

- ISO 27005 - Norma adaptada à Gestão de Risco de Segurança da Informação

- Alinhada com o modelo PDCA da ISO 27001





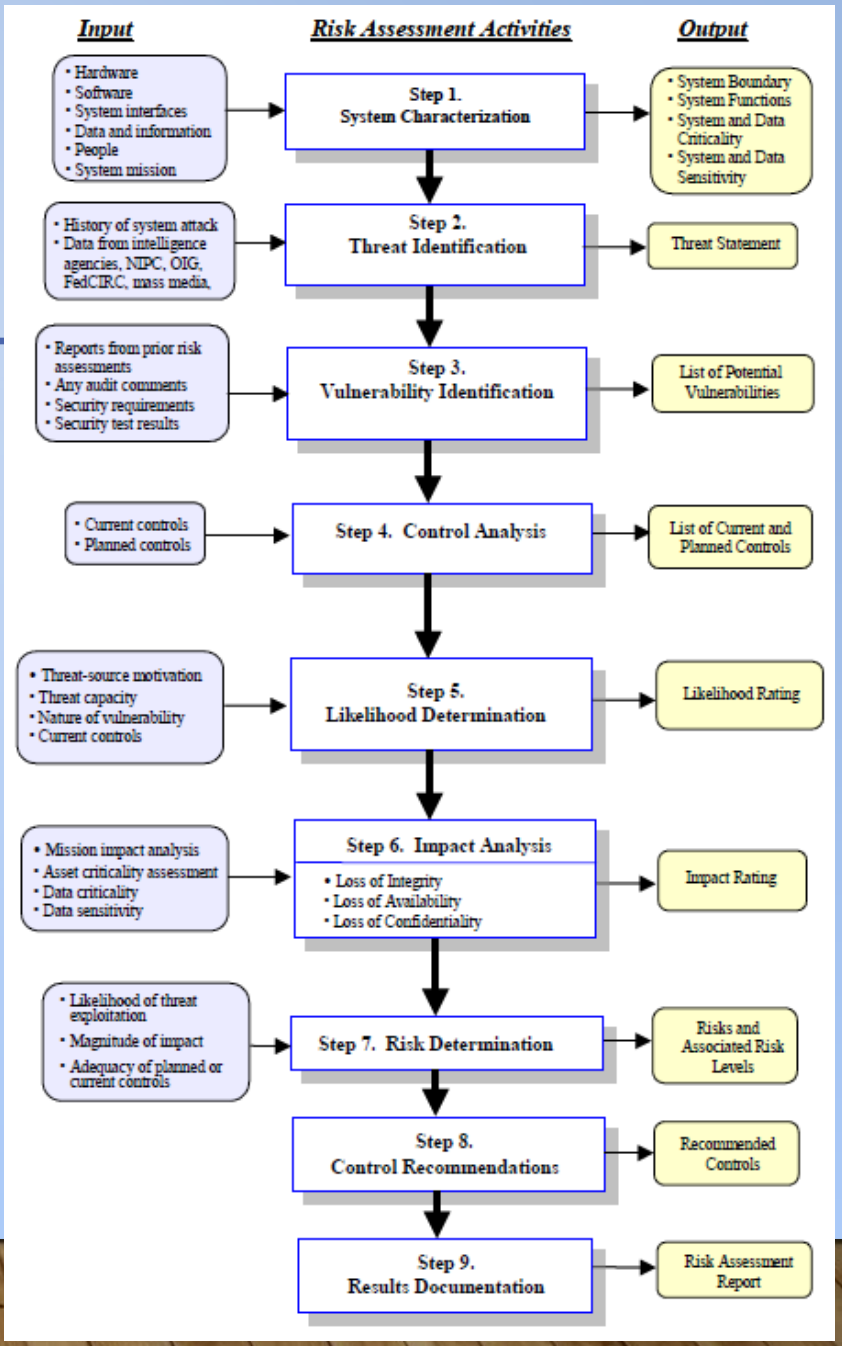
23 A AVALIAÇÃO E GESTÃO DOS RISCOS

- ERM / COSO - Enterprise Risk Management, do COSO (Committee of Sponsoring Organizations of the Treadway Commission)
  - Componentes ERM
    - cruzando categorias de objetivos (estratégicos, operacionais, de comunicação e conformidade) com a Organização (nível de organização, divisão, unidade de negócio e subsidiária)

A AVALIAÇÃO E GESTÃO DOS RISCOS

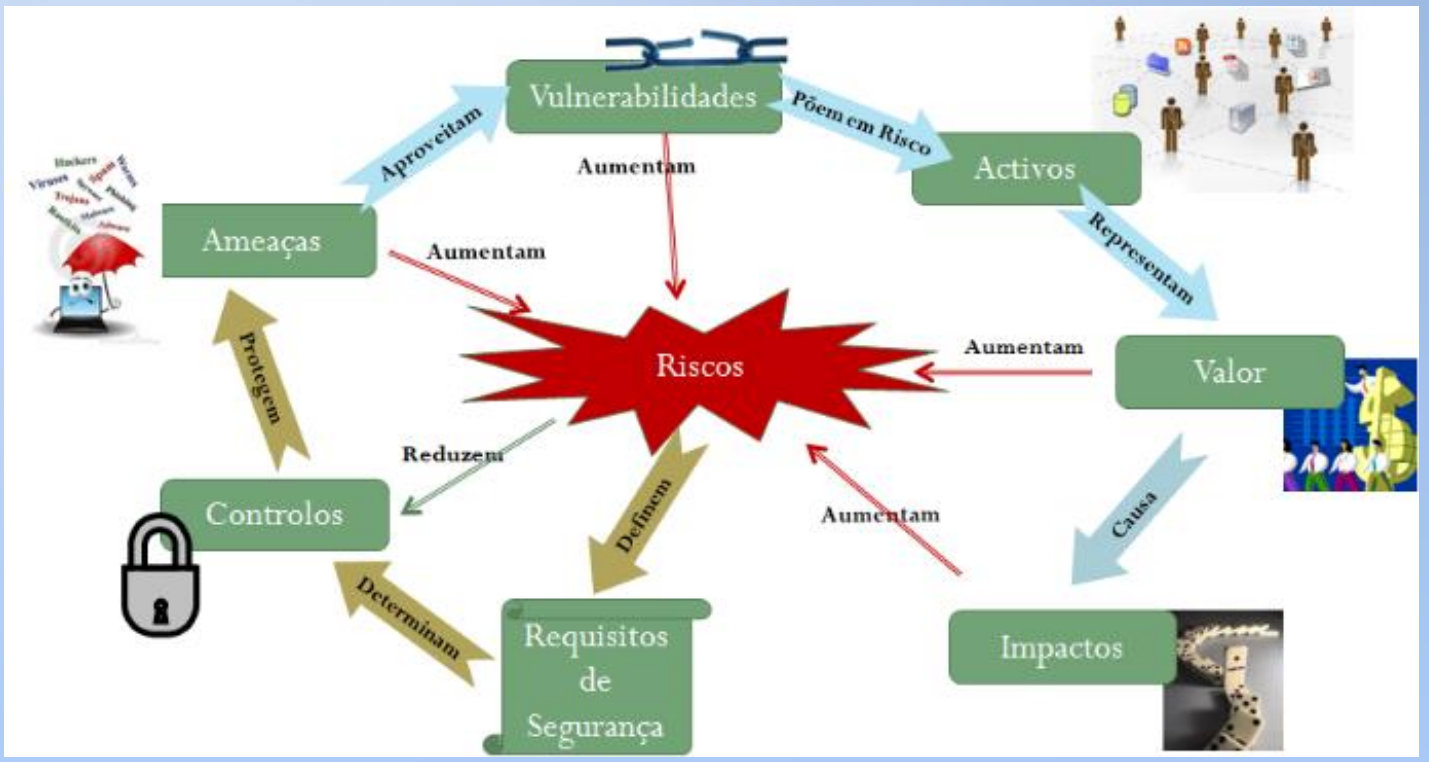
- As etapas de uma Avaliação de Riscos (segundo o NIST - National Institute of Standards and Technology)
  - Caracterização do sistema
  - Identificação das ameaças
  - Identificação das Vulnerabilidades
  - Análise de controlos
  - Determinação de probabilidades
  - Análise de impacto
  - Determinação do Risco
  - Recomendação de Controlos a implementar
  - Documentação final

  Apresenta pormenores cuja adoção poderá beneficiar a metodologia a adotar
- (NIST SP800-30 - Risk Management Guide for IT Systems)



25 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Mas:
  - Como quantificar o Risco?
  - Como estimar a probabilidade?
  - Como avaliar o Risco?

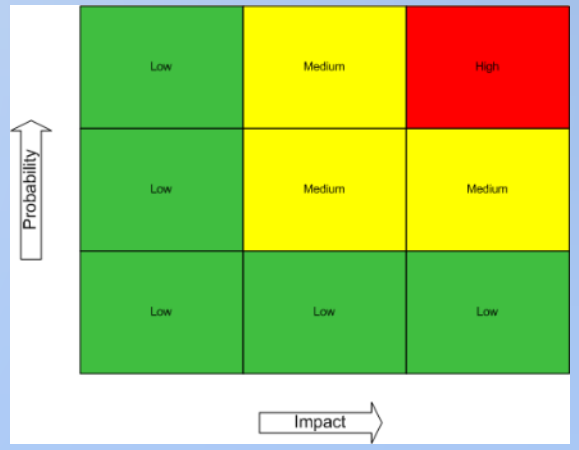


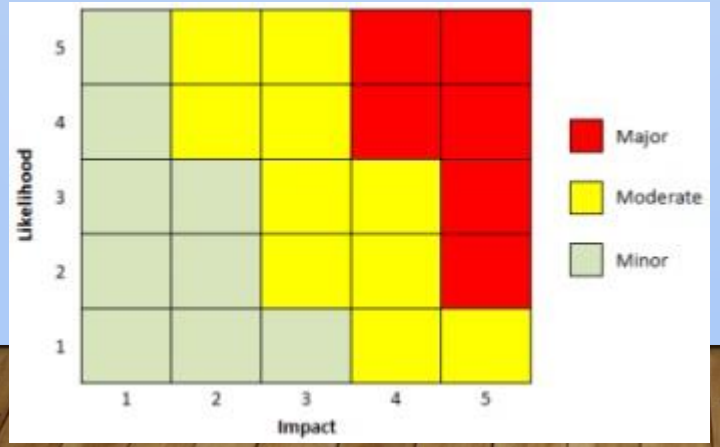
26 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Formas de quantificar o Risco?
- Avaliação quantitativa, recorrendo a valores numéricos

	Matriz de Probabilidade x Impacto				
Probabilidade					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Impacto	1	2	3	4	5

- Avaliação qualitativa, através de níveis de valores, utilizando categorias e níveis de risco
- Ou uma avaliação mista





27 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Formas de quantificar o Risco?
  - Avaliação qualitativa vs Avaliação quantitativa

> "Many discussions of security risk analysis methodologies mention a distinction between quantitative and qualitative risk analysis, but virtually none of those discussions clarify the distinction in a rigorous way"
>
> (Posted By Jeff Lowder On September 4, 2008 @ 6:00 am In Risk Analysis)

- Quantitative Risk Analyses assign fixed numerical values (within a margin of error) to both the probability and utility (business impact) of an outcome;

- Qualitative Risk Analyses don't. Instead, they represent both the probability and utility of an outcome using an interval scale, where each interval includes a range of numerical values (beyond the margin of error) and each interval is typically represented by a non-numerical label (such as the words "High", "Medium", "Low"), not the ranges of values those labels represent.

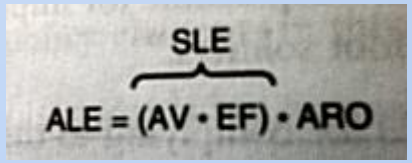
28 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Avaliação de risco
  - Existem várias formas de calcular o risco
    - Em função da metodologia adoptada
    - No entanto, tem que ser sistemática e repetível
  - Alguns exemplos de fórmulas de cálculo de risco:
    - Risco = Probabilidade x Consequência x Severidade
    - Risco = Valor_Ativo x Probabilidade x Impacto
    - Risco = Probabilidade x Impacto
  - Preferencialmente, devem ser utilizados valores quantitativos (1, 2, 3, 4, 5) em vez de qualitativos (alto, médio, baixo)
    - A ISO27005 refere:

"Qualitative risk analysis may be used:
- As an initial screening activity to identify risks that require more detailed analysis
- Where this kind of analysis is appropriate for decisions
- Where the numerical data or resources are inadequate for a quantitative risk analysis"

29 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Avaliação quantitativa, recorrendo a valores monetários



- SLE – Single Loss Expectancy
- ALE – Annualized Loss Expectancy
- ARO – Annualized Rate of Occurrence
- AV – Asset value
- EF – Exposure Factor: % Loss that is expected to occur.

Asset Value (AV)	2000000	Replacement / Recovery / Reporting /
Exposure Factor (EF)	75.00%	Percentage of asset loss caused by identified threat (Single Event)
Single Loss Expectancy (SLE)	1500000	AV x EF
Annualized Rate of Occurance (ARO)	0.02	Estimated frequency a threat will occur (or fraction thereof)..
Annualized Loss Expectancy (ALE)	30000	SLE x ARO

A AVALIAÇÃO E GESTÃO DOS RISCOS

- Avaliação quantitativa
  - Através da aplicação deste método, os fatores do risco (probabilidade e severidade) são classificados através da atribuição de um valor (numérico ou verbal) que está integrado numa escala de valores relativos.
  - Cada valor da escala é associado a uma descrição explicativa.
    - Mas atenção à subjetividade

1	Raramente	Pouco credível que alguma vez aconteça
2	Improvável	Pode ocorrer ocasionalmente
3	Possivelmente	É possível que aconteça, mas não é esperado
4	Provavelmente	Provavelmente irá acontecer
5	Quase certo	Acontecerá com alguma frequência

A AVALIAÇÃO E GESTÃO DOS RISCOS

- Avaliação quantitativa

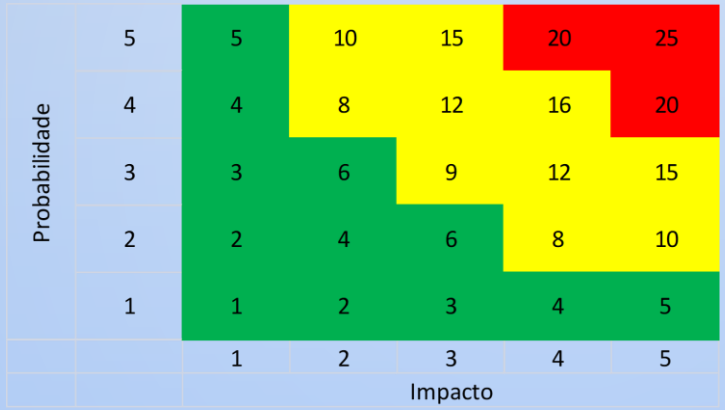
- Considerados níveis de avaliação de 1 a 5

- Neste caso o Risco é de 45, considerando:
- o valor de 5 para o activo
- 3 para a probabilidade da ameaça se concretizar
- e 3 para o impacto da vulnerabilidade

Risk	Valor
Asset	
Dados de Clientes	5
Threat	
Roubo de informação interno	3
Vulnerability	
Dados em claro na Base de dados (apesar de controlo de acessos)	3
Total	45

32 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Exemplo de cálculo de risco



Probabilidade		
Níveis	**Probabilidade**	**Ocorrências por ano**
Nível 1	Improvável	0 a 1 vez
Nível 2	Pouco provável	1 a 2 vezes
Nível 3	Provável	2 a 3 vezes
Nível 4	Bastante provável	3 a 4 vezes
Nível 5	Muito Provável	Mais de 4

Impacto		
Níveis	**Impacto**	**Descrição do nível de impacto**
Nível 1	Muito Baixo	Um posto de trabalho parado
Nível 2	Baixo	Um sistema/processo parado
Nível 3	Médio	Um departamento parado
Nível 4	Alto	Mais que um departamento parado
Nível 5	Muito alto	A organização pára completamente

	Actual				Mitigação			
	Actual				Mitigação			
	Actual				Mitigação			
Risco = função(Ameaça,vulnerabilidade, consequência)	Controlos Existentes	Probabilidade	Impacto	Valor Risco = P * I	Novo Controlo	Probabilidade2	Impacto2	Novo Risco = P2 * I2
Acesso de colaboradores a documentos classificados, por privilégios mal configurados	-	3	5	15	implementar serviços de directório, com controlo de acessos por perfil	1	5	5

A AVALIAÇÃO E GESTÃO DOS RISCOS

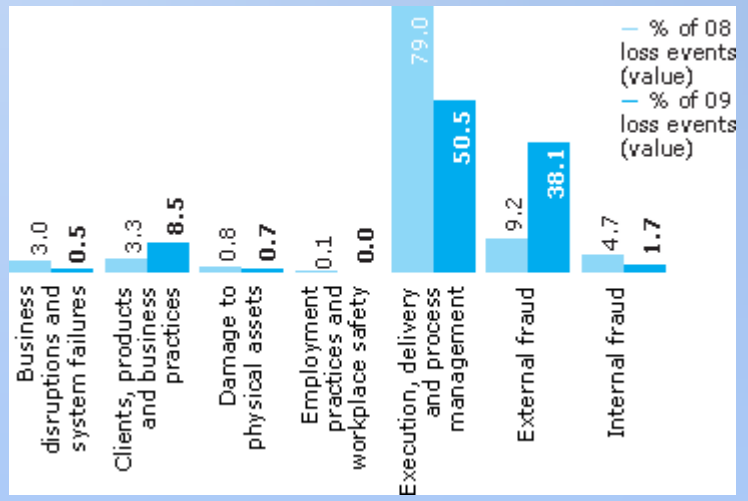
- Formas de estimar a probabilidade
  - Através de dados e input interno
  - Recorrendo a dados externos

34 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Estimar a probabilidade através de dados e inpust internos
  - Utilizar histórico dos incidentes para determinar os riscos actuais
    - Carece de mecanismos de recolha e análise de dados
      - IDS, CSIRT (Computer Security Incident Response Team), Security Event Correlation and Analysis…
    - Pressupõe que os dados recolhidos são representativos
    - Pressupõe padrão semelhante de comportamento no futuro
  - Recorrer ao conhecimento e experiência dos colaboradores e especialistas internos em segurança
  - Através de metodologias estruturadas de recolha de dados:
    - Com questionários;
    - E discussões de grupo.

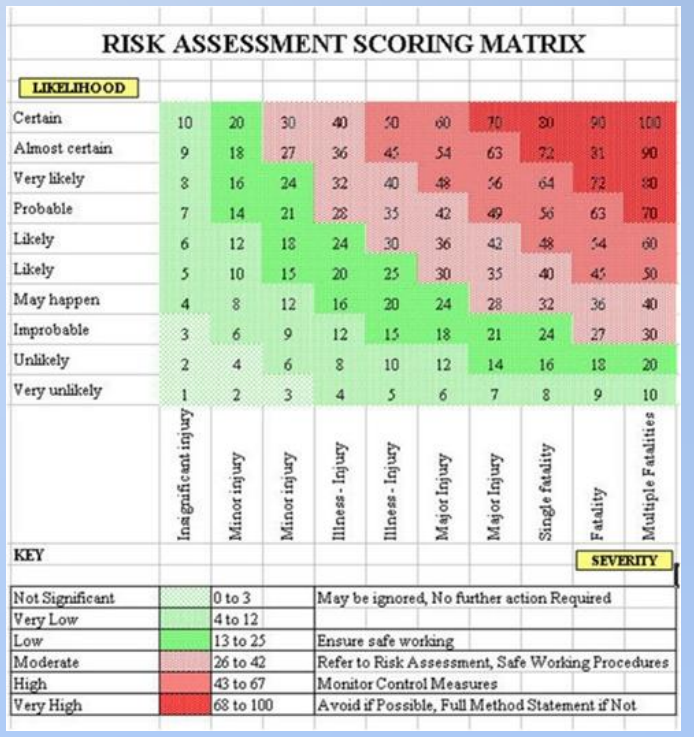
35 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Estimar a probabilidade através de dados externos
  - Dados partilhados por outras organizações
    - Pressupõe uma exposição ao risco semelhante
    - Implica analisar e escolher com cuidado uma amostra representativa
  - Recorrer a dados partilhados por
    - Information Security Forum (ISF)
    - Operational Riskdata eXchange Association
    - …
    - Ou relatórios de entidades privadas
      como barclaysannualreport.com



36 A AVALIAÇÃO E GESTÃO DOS RISCOS

- Avaliar o Risco
  - Analisando a gravidade do risco
  - O nível de aceitação do risco pode ser estabelecido pela intersecção da escala da probabilidade e severidade.
  - No exemplo o nível de aceitação do risco é 25.
  - Riscos estimados com valores superiores a 68 são considerados intoleráveis, devendo ser evitados.



RISK ASSESSMENT SCORING MATRIX

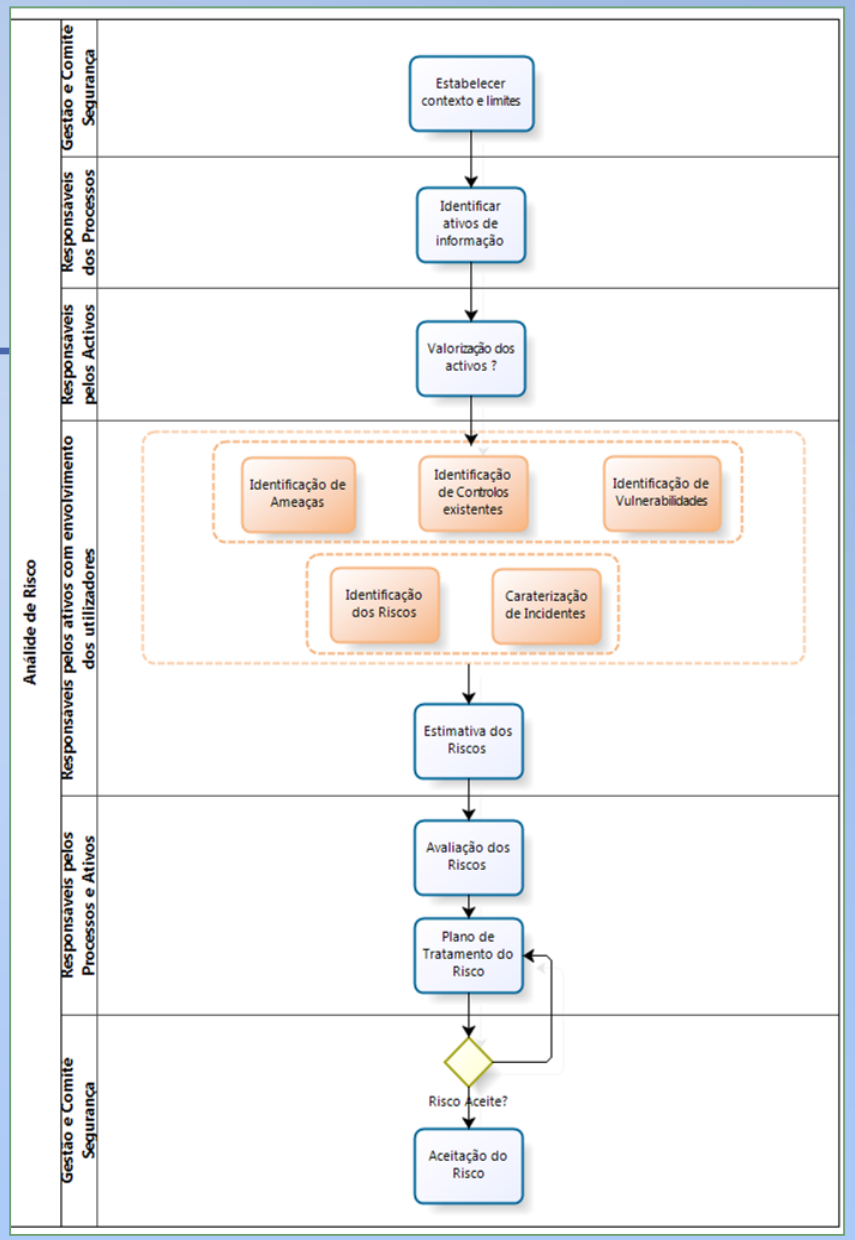
LIKELIHOOD										
Certain	10	20	30	40	50	60	70	80	90	100
Almost certain	9	18	27	36	45	54	63	72	81	90
Very likely	8	16	24	32	40	48	56	64	72	80
Probable	7	14	21	28	35	42	49	56	63	70
Likely	6	12	18	24	30	36	42	48	54	60
Likely	5	10	15	20	25	30	35	40	45	50
May happen	4	8	12	16	20	24	28	32	36	40
Improbable	3	6	9	12	15	18	21	24	27	30
Unlikely	2	4	6	8	10	12	14	16	18	20
Very unlikely	1	2	3	4	5	6	7	8	9	10
	Insignificant injury	Minor injury	Minor injury	Illness - Injury	Illness - Injury	Major Injury	Major Injury	Single fatality	Fatality	Multiple Fatalities

SEVERITY

KEY			
Not Significant		0 to 3	May be ignored, No further action Required
Very Low		4 to 12	
Low		13 to 25	Ensure safe working
Moderate		26 to 42	Refer to Risk Assessment, Safe Working Procedures
High		43 to 67	Monitor Control Measures
Very High		68 to 100	Avoid if Possible, Full Method Statement if Not

ANÁLISE E AVALIAÇÃO DE RISCO

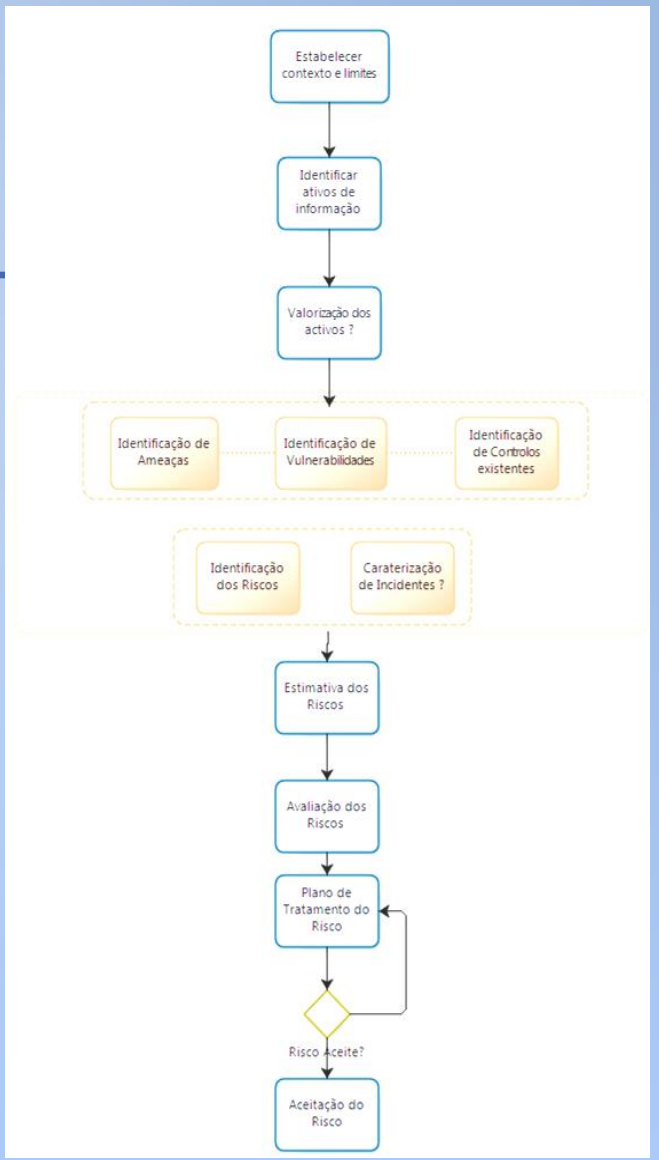
- Detalhe do processo de Análise e Avaliação de Risco
  - Baseado na ISO27005



ANÁLISE E AVALIAÇÃO DE RISCO

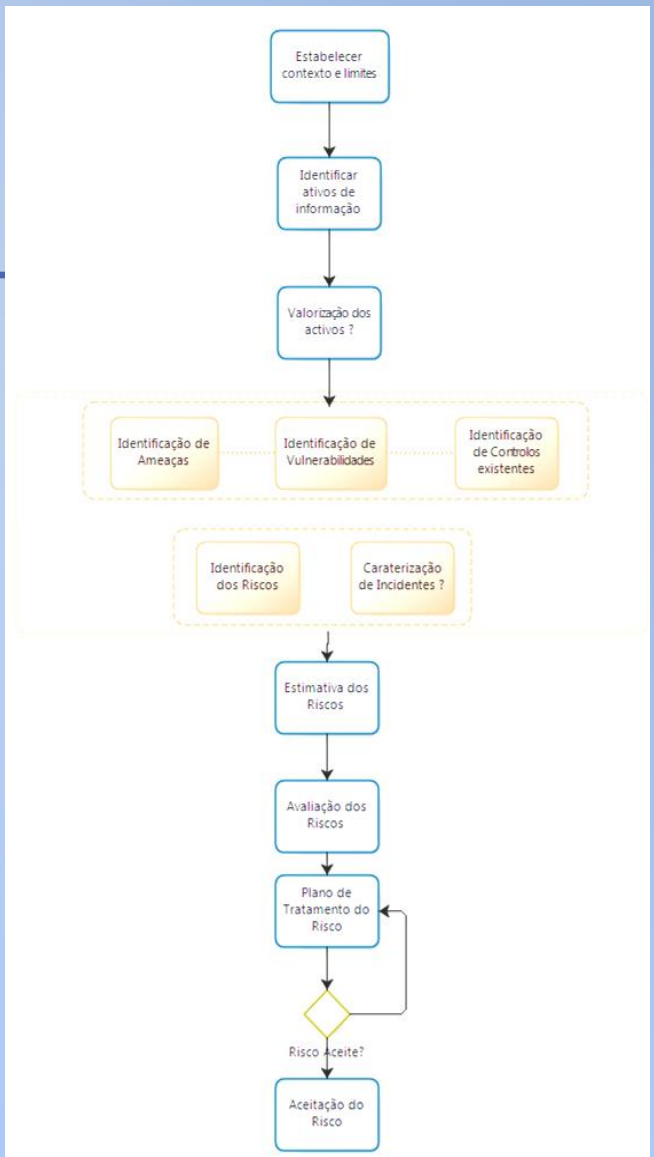
- Estabelecer o contexto e limites
  - Caracterizar as atividades e processos de negócio que se encontram dentro do âmbito do SGSI, bem como identificar os pontos de contato com outras atividades e processos com os quais interagem.

- Definir os princípios orientadores para a análise e avaliação dos riscos:
  - Forma e níveis de avaliação a serem utilizados;
    - Formula de estimativa de riscos
    - Níveis e descrição dos critérios de avaliação da fórmula
  - Valor mínimo dos ativos a abranger na análise de risco;
  - Valor do Risco aceitável, acima do qual requer o tratamento do risco.



39 ANÁLISE E AVALIAÇÃO DE RISCO

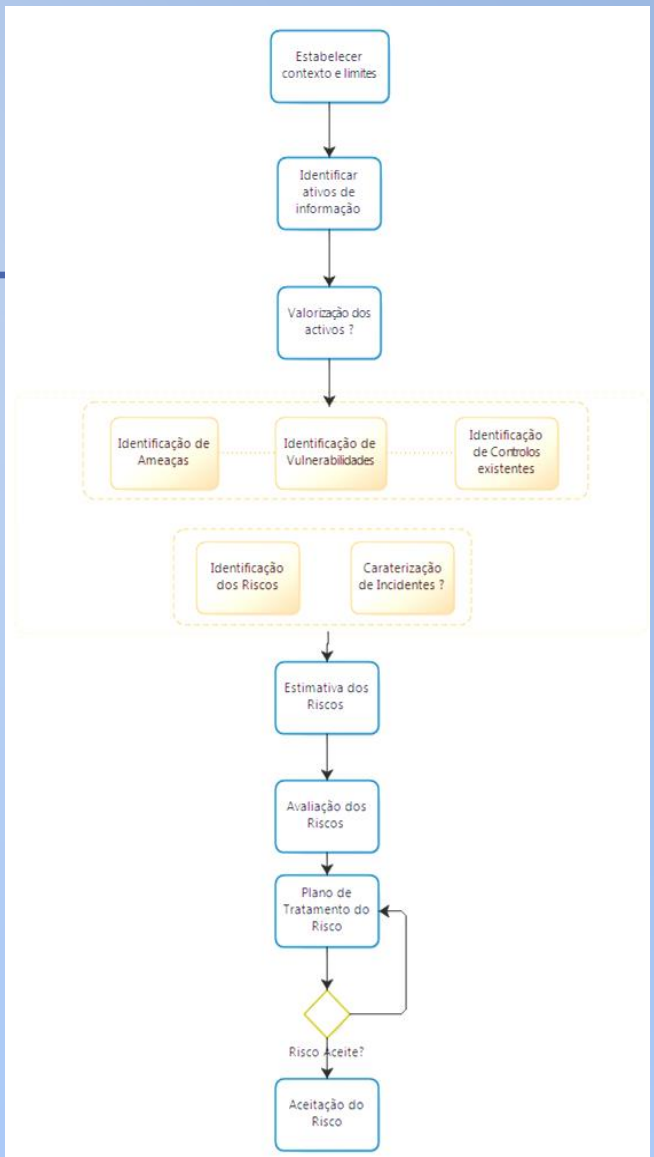
- Identificação dos Ativos de Informação
  - Identificar todos os ativos relevantes, com informação
    - Nome
    - Descrição
    - Tipo de Ativo
    - Responsável
    - Localização
    - Dependências (de outros ativos)
  - Agrupar por tipos de ativos:
    - Instalações
    - Equipamentos e Dispositivos Informáticos
    - Outros Equipamentos
    - Software de Base (S.O:, SGBD, ERP, ..)
    - Software Aplicacional
    - Informação lógica
    - Informação Física
    - Colaboradores Internos
    - Colaboradores Externos
    - Serviços externos de suporte
    - Ativos organizacionais



ANÁLISE E AVALIAÇÃO DE RISCO

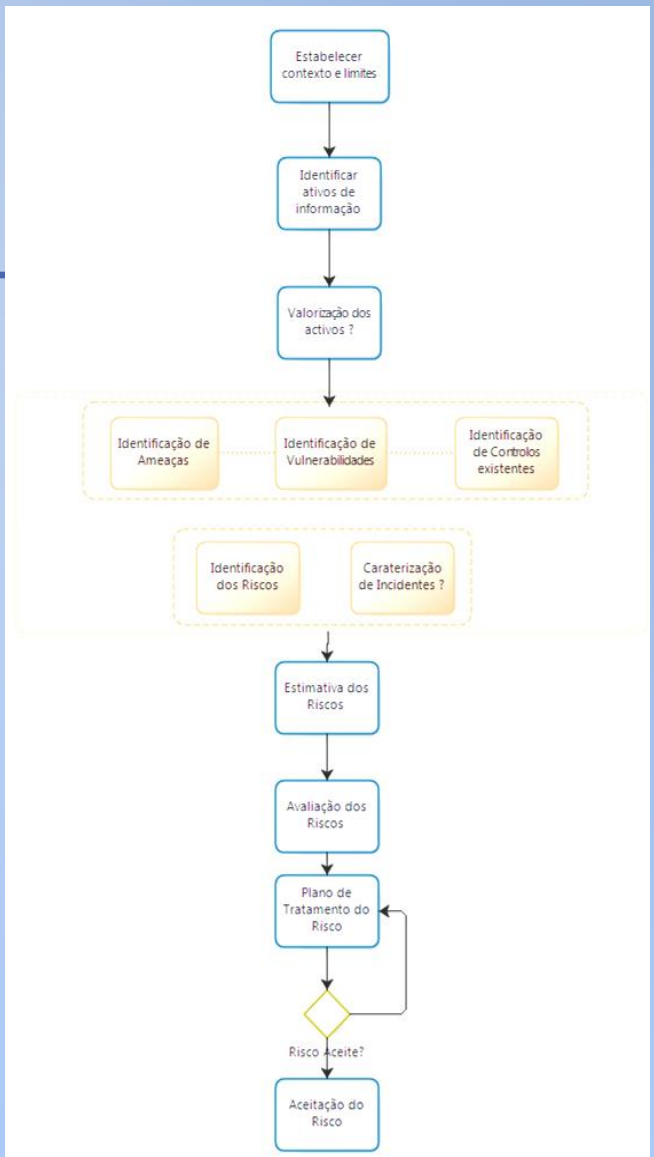
- Valorização dos Ativos
  - Atribuição de um nível de valor (numa escala de 1 a 4) para cada ativo, em função da sua importância comercial ou operacional
  - Triagem dos ativos que carecem de análise de risco, em função do seu valor
    - p.e. só analisar ativos de valor Médio, Alto ou Muito Alto

Valor	Descrição
4	**Muito Alto** O processo não se executará conforme o estipulado, comprometendo acordos comerciais
3	**Alto**. O processo não se executará conforme o estipulado,
2	**Médio**. O processo será executado, mas existirão impactos negativos na operação
1	**Baixo**. O processo executará normalmente, podendo existir pequenos impactos na operação



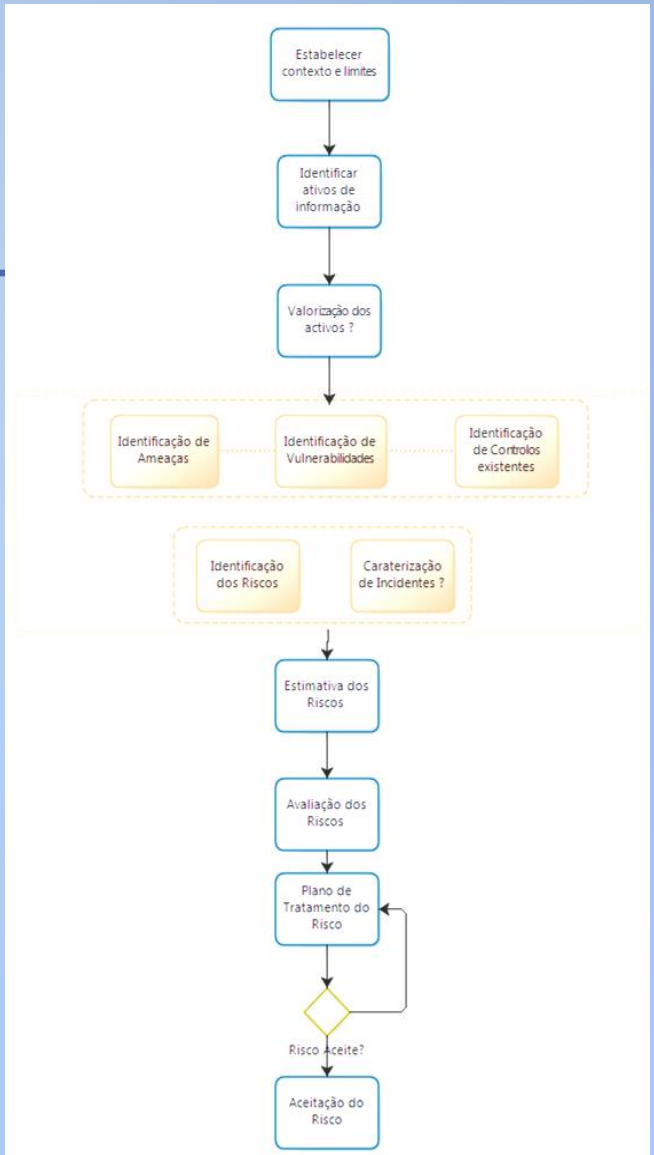
ANÁLISE E AVALIAÇÃO DE RISCO

- Identificação de Ameaças
  - Por tipo de Ativo
- Identificação de Vulnerabilidades
  - Por Tipo de Ativo
- Identificação de Controlos existentes
  - Por tipo de ativo
  - Verificar listagem de controlos da norma ISO27001
- Identificação de Riscos
  - O risco como a consequência de uma ameaça explorar uma vulnerabilidade
  - Depois de identificadas as ameaças e riscos devem ser encontrados os pares Ameaça+Vulnerabilidade que façam sentido
  - Estes Ameaça+Vulnerabilidade devem estar associados a vários tipos de ativos
- Caraterização de Incidentes
  - Quando a possibilidade de concretização de uma ameaça+vulnerabilidade resulta num conjunto de riscos



ANÁLISE E AVALIAÇÃO DE RISCO

- Estimativa dos Riscos
- Estimar a probabilidade de um risco se concretizar
- Risco Operacional
  - Estimar o impacto operacional de um risco se concretizar
  - Impacto operacional – indisponibilidade do(s) serviço(s)
  - Calcular o valor do Risco (O) = Probabilidade * Impacto Operacional
- Risco Financeiro
  - Estimar Impacto financeiro em valor monetário
  - Impacto financeiro = perdas financeiras decorrentes de ocorrências e de reposição da atividade normal
- Calcular o valor do Risco (F) = Probabilidade * Impacto Financeiro
- Escolher o maior nível de risco

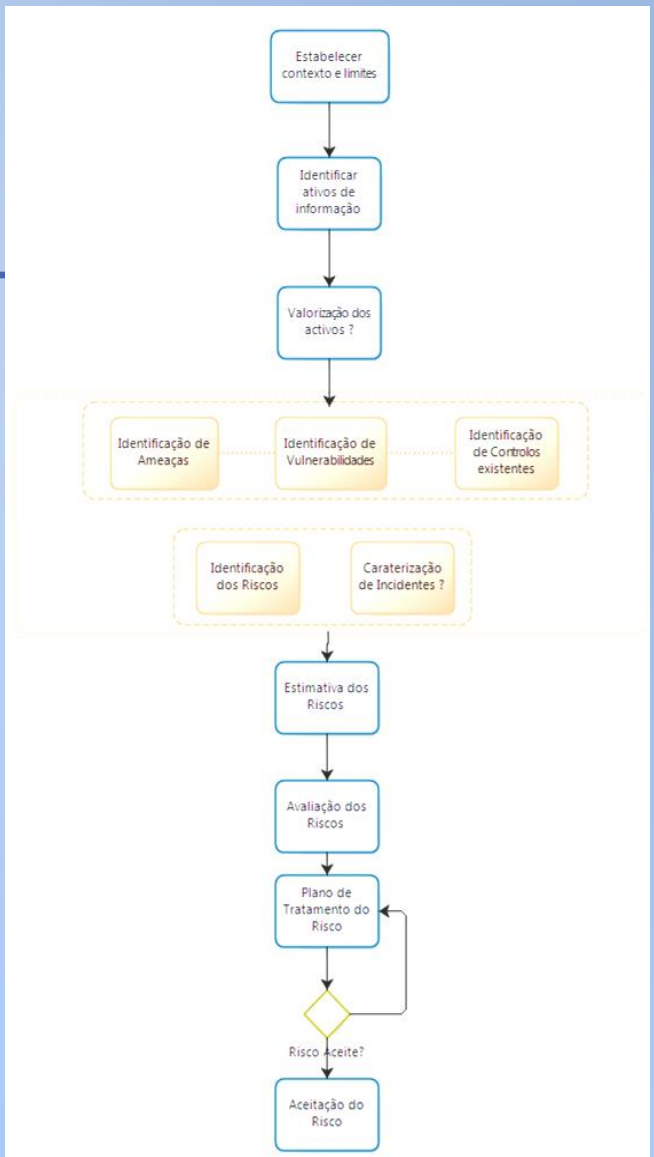


ANÁLISE E AVALIAÇÃO DE RISCO

- Avaliação dos Riscos
  - Identificar os riscos que se encontram dentro dos limites aceitáveis e os que carecem tratamento

- Plano de Tratamento do Risco
  - Identificar as formas de tratamento dos riscos
  - Caracterizar os controlos a implementar, por forma a reduzir os riscos a valores aceitáveis, reavaliando os riscos

- Aceitação do Risco
  - Aceitação pela gestão dos riscos e do plano de tratamento traçado



44 AGENDA

- Introdução à Gestão de Continuidade de Negócio
- A avaliação e gestão de riscos
- **Tratamento dos Riscos**
- Controlos de segurança
  - Tecnológicos, Operacionais e de Gestão

TRATAMENTO DOS RISCOS

- Opções de Tratamento de Risco (ISO27005/Segurança da Informação)
  - Assumir o Risco
    - Aceitar o Risco continuando com o sistema em operação
    - Podendo/devendo ir implementando controlos tendentes à redução do risco
  - Evitar o Risco
    - Eliminando a causa do risco ou as consequências (desactivar certas funcionalidades ou,mesmo, desligar o sistema)
  - Transferência de Risco
    - Utilizando opções que permitam cpmpensação em caso de perdas (p.e. seguros)
  - Aplicação de Controlos ou Mitigação dos Riscos
    - Controlos de segurança apropriados às ameaças e vulnerabilidades encontradas no sentido de reduzir o risco final

TRATAMENTO DOS RISCOS

- Opções de Tratamento de Risco (ISO 31000)
  - "As opções para o tratamento do risco poderão envolver uma ou mais das seguintes opções:
    - evitar o risco ao decidir não iniciar ou continuar com a atividade que origina o risco;
    - aceitar ou aumentar o risco de modo a explorar uma oportunidade;
    - remover a fonte do risco;
    - alterar a verosimilhança;
    - alterar as consequências;
    - partilhar o risco (p.e. através de contratos, aquisição de seguros);
    - reter o risco mediante decisão informada

47 TRATAMENTO DOS RISCOS

- Opções de Tratamento dos Riscos (NIST)
  - Assumir o Risco
    - Aceitar o Risco continuando com o sistema em operação
    - Podendo/devendo ir implementando controlos tendentes à redução do risco
  - Evitar o Risco
    - Eliminando a causa do risco ou as consequências (desativar certas funcionalidades ou, mesmo, desligar o sistema)
  - Transferência de Risco
    - Utilizando opções que permitam compensação em caso de perdas (p.e. seguros)
  - Planeamento de Risco
    - Gerir o risco, desenvolvendo um plano de mitigação que prioriza, implementa e mantem os controlos
  - Limitar o Risco
    - Implementar os controlos capazes de minimizar o impacto de certas ameaças sobre alguma vulnerabilidade
    - Necessário implementar medidas de detecção, prevenção e suporte
    - (se for verificado um determinado incidente, desligar sistema, ou repor sistema…)
  - Reconhecimento e Desenvolvimento de controlos
    - De forma a baixar o risco, à medida que as vulnerabilidades são reconhecidas, é implementado um plano de desenvolvimento e implementação de controlos que permitam corrigir ou minimizar a vulnerabilidade

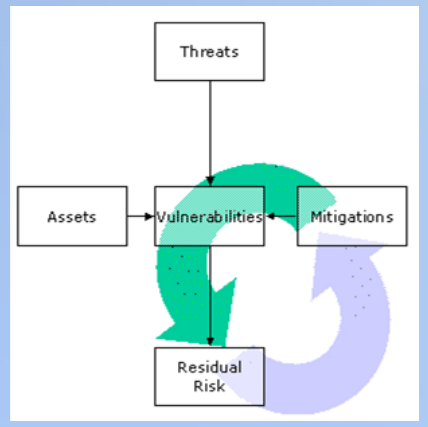
TRATAMENTO DOS RISCOS - TÉCNICO E/OU ADMINISTRATIVO

- Mitigação técnica ou administrativa ?
- Assumir o Risco
- Evitar o Risco
- Transferência de Risco
- Planeamento de Risco
- Limitar o Risco
- Reconhecimento e Desenvolvimento de controlos

Predominantemente técnicos

49 TRATAMENTO DOS RISCOS

- Risk Mitigation Checklist (extraído do NIST)
  - Each proposed risk mitigation option should be examined from the following perspectives:
    - Effectiveness.
      - Will it reduce or eliminate the identified risks? To what extent do alternatives mitigate the risks? Effectiveness can be viewed as being somewhere along a continuum, as follows:
        - Level One (Engineering actions): The safety action eliminates the risk, for example, by providing interlocks to prevent thrust reverser activation in flight;
        - Level Two (Control actions): The safety action accepts the risk but adjusts the system to mitigate the risk by reducing it to a manageable level, for example, by imposing more restrictive operating conditions; and
        - Level Three (Personnel actions): The safety action taken accepts that the hazard can neither be eliminated (Level One) nor controlled (Level Two), so personnel must be taught how to cope with it, for example, by adding a warning, a revised checklist and extra training.

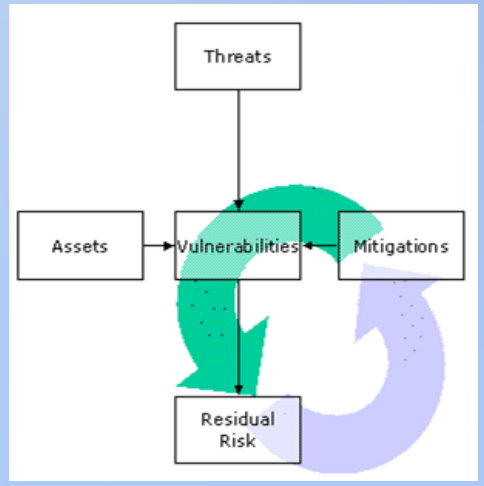


TRATAMENTO DOS RISCOS

- Cost/benefit.
  - Do the perceived benefits of the option outweigh the costs? Will the potential gains be proportional to the impact of the change required?
- Practicality.
  - Is it doable and appropriate in terms of available technology, financial feasibility, administrative feasibility, governing legislation and regulations, political will, etc.?
- Challenge.
  - Can the risk mitigation measure withstand critical scrutiny from all stakeholders (employees, managers, stockholders/State administrations, etc.)?
- Acceptability to each stakeholder.
  - How much buy-in (or resistance) from stakeholders can be expected? (Discussions with stakeholders during the risk assessment phase may indicate their preferred risk mitigation option.)

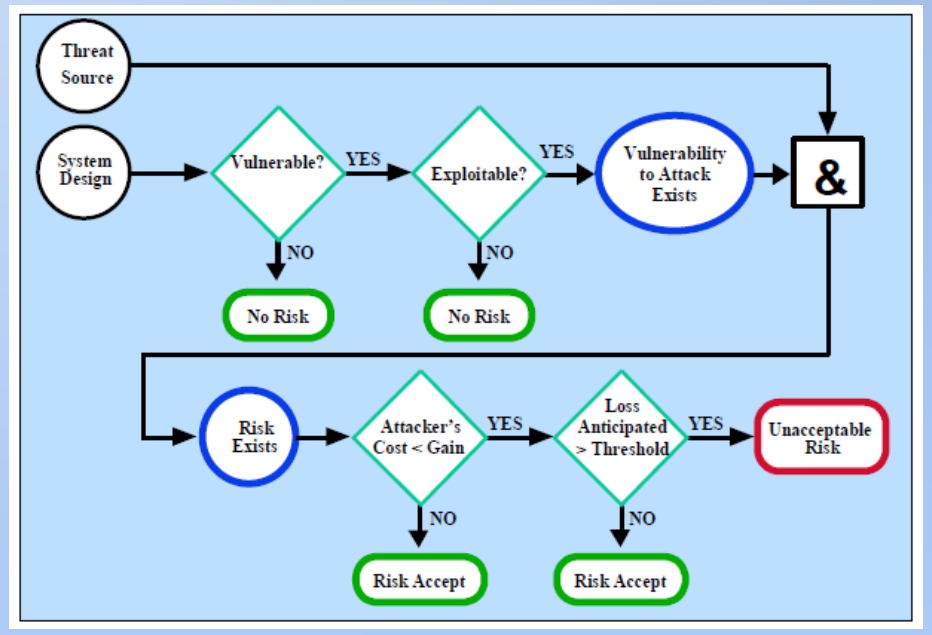
TRATAMENTO DOS RISCOS

- Enforceability.
  - If new rules (SOPs, regulations, etc.) are implemented, are they enforceable?
- Durability.
  - Will the measure withstand the test of time? Will it be of temporary benefit or will it have long-term utility?
- Residual risks.
  - After the risk mitigation measure is implemented, what will be the residual risks relative to the original hazard? What is the ability to mitigate any residual risks?
- New problems.
  - What new problems or new (perhaps worse) risks will be introduced by the proposed change?



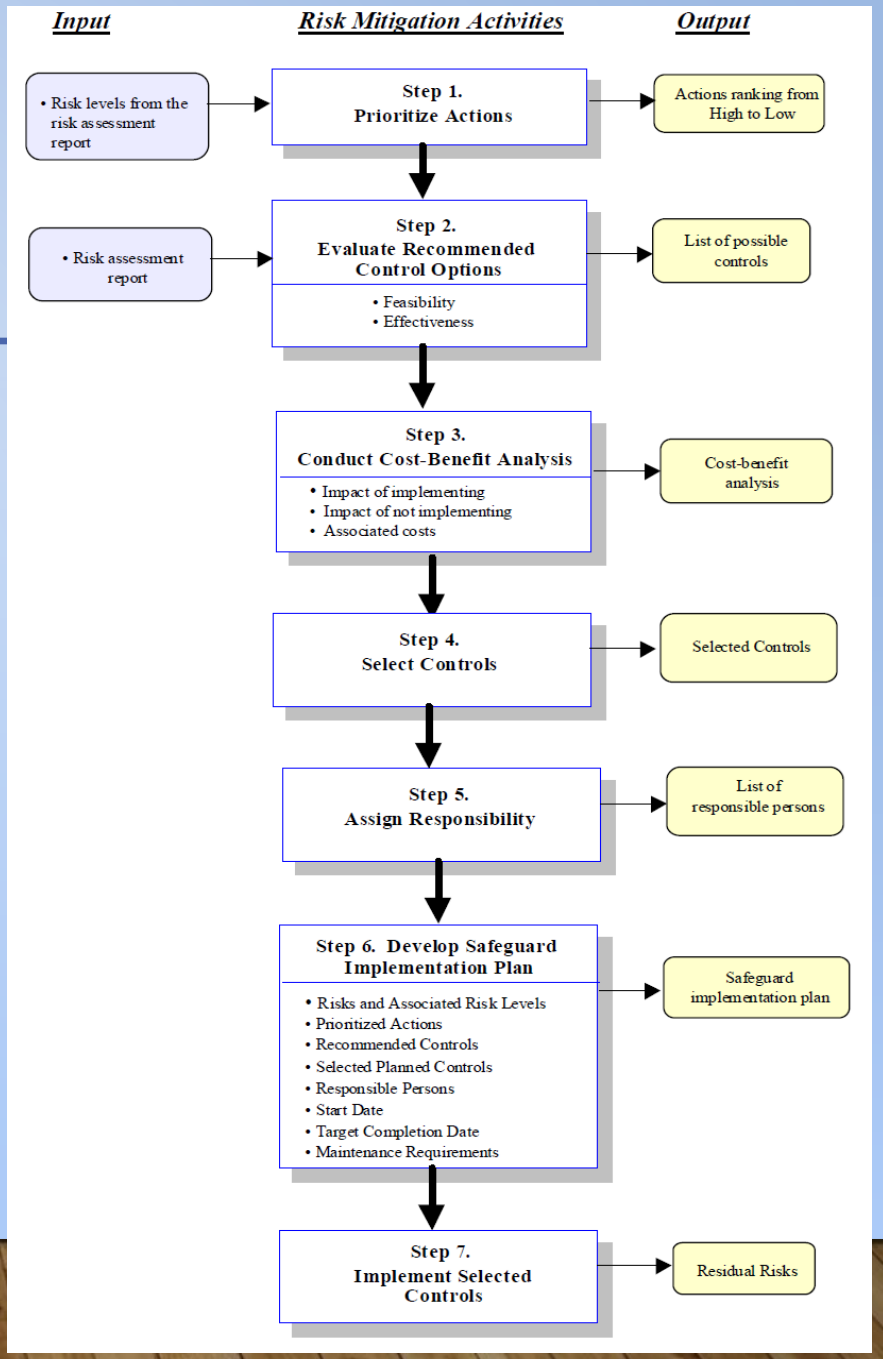
52 TRATAMENTO DOS RISCOS

- Fluxo de aceitação de riscos
- Ou não aceitação e implementação de controlos



TRATAMENTO DOS RISCOS

- 7 passos para a implementação de controlos
  - Step 1- Prioritize Actions
    - Output -Actions ranking from High to Low
  - Step 2- Evaluate Recommended Control Options
    - Output from - List of feasible controls
  - Step 3 - Conduct Cost-Benefit Analysis
    - Output - Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls
  - Step 4 - Select Control
    - Output from - Selected control(s)
  - Step 5 - Assign Responsibility
    - Output - List of responsible persons
  - Step 6 - Develop a Safeguard Implementation Plan
    - Output - Safeguard implementation plan
  - Step 7 - Implement Selected Control(s)
    - Output from - Residual risk



54 AGENDA

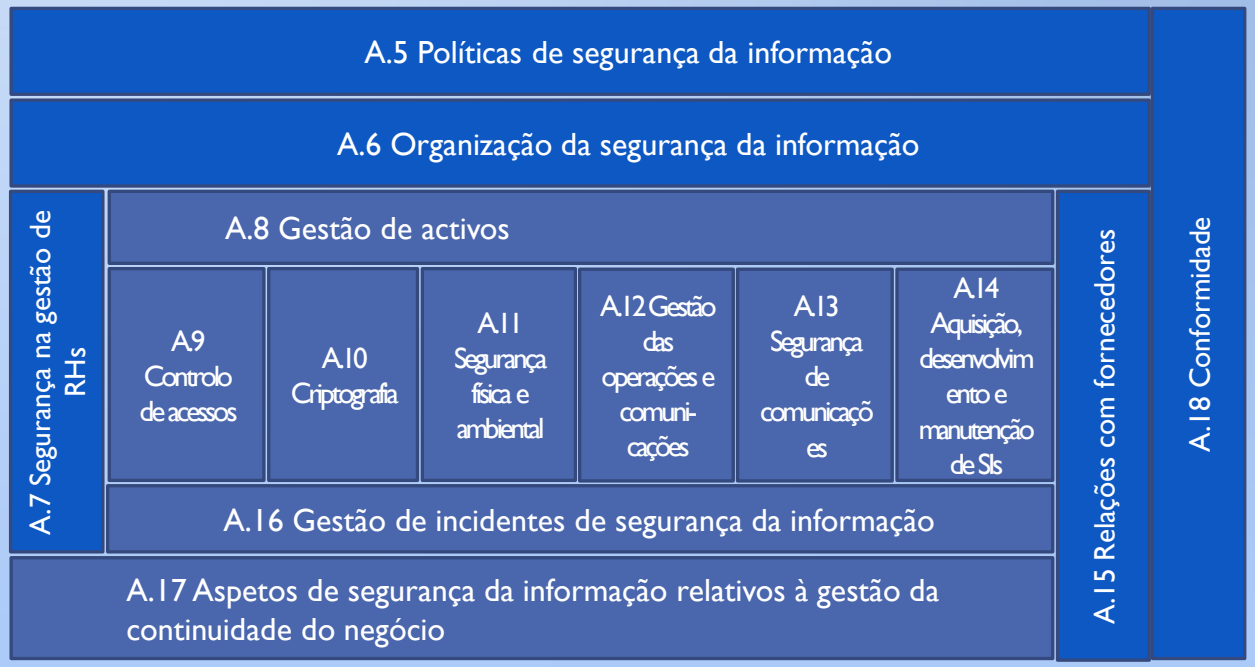
- Introdução à Gestão de Continuidade de Negócio
- A avaliação e gestão de riscos
- Tratamento dos Riscos
- **Controlos de segurança**
  - **Tecnológicos, Operacionais e de Gestão**

55 CONTROLOS DE SEGURANÇA

- A implementação de controlos ou medidas de segurança
  - Deve resultar de um processo de avaliação de riscos
  - Opção de Tratamento Técnico ou Administrativo
    - Compromisso entre ambas
  - Carece de uma cuidada análise de custo-benefício

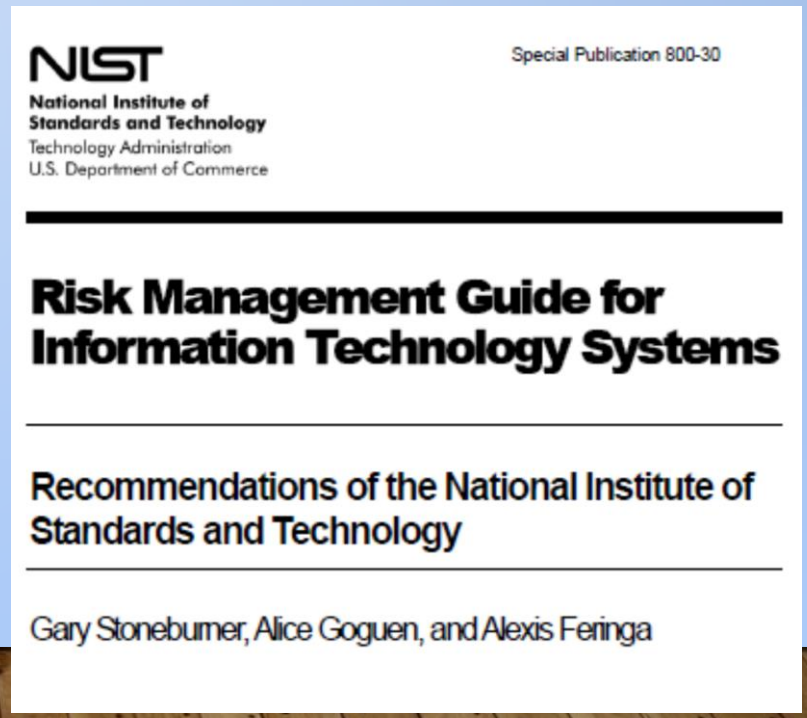
56 CONTROLOS DE SEGURANÇA

- Na ISO/IEC 27001 os controlos de segurança estão agrupados em 14 pontos, do Anexo A
  - Administrativos e de procedimento
  - tecnológicos



57 CONTROLOS DE SEGURANÇA

- Os controlos a implementar podem ser agrupados em (NIST Special Publication 800-30)
  - Tecnológicos
  - Não tecnológicos: Gestão,
  - Operacionais e Organizacionais


NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-30

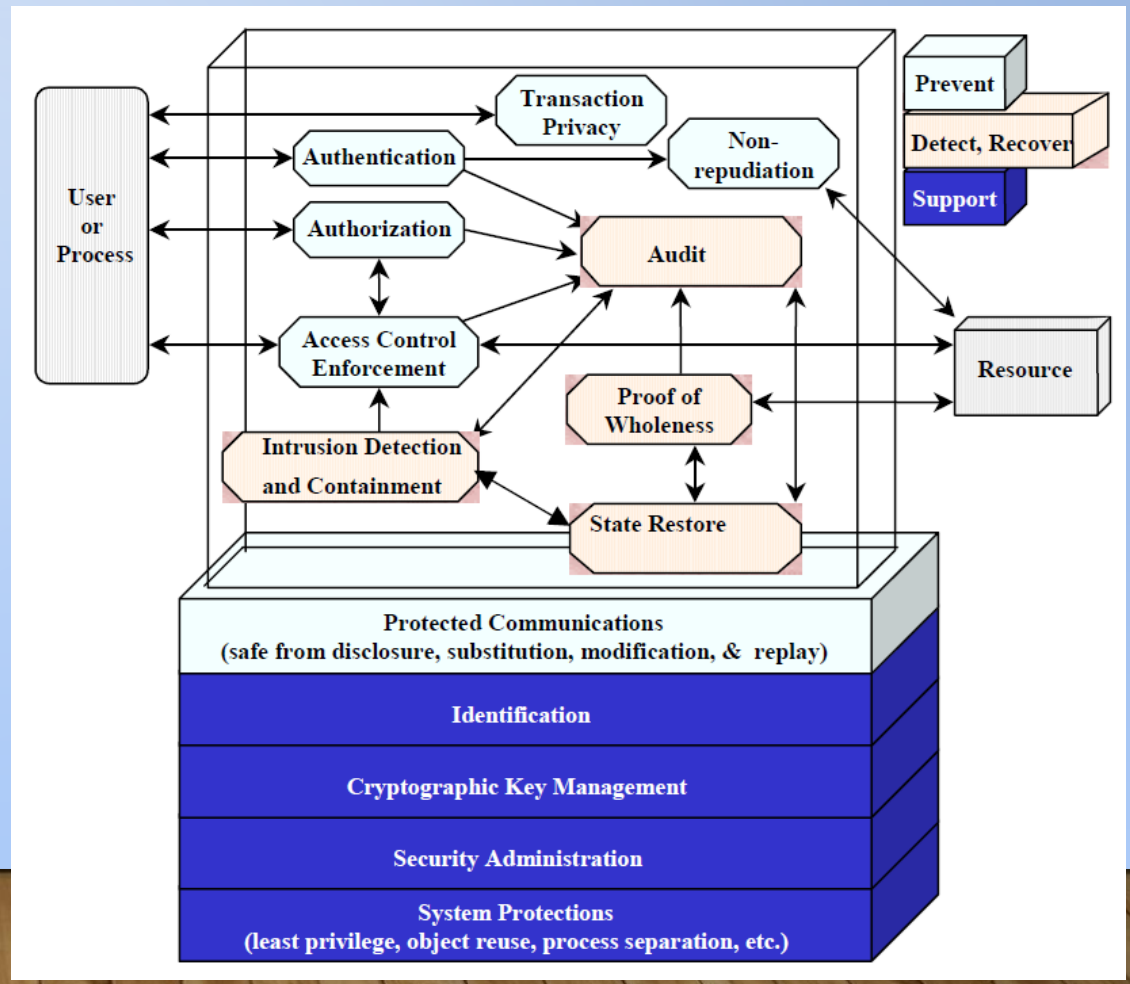
Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa

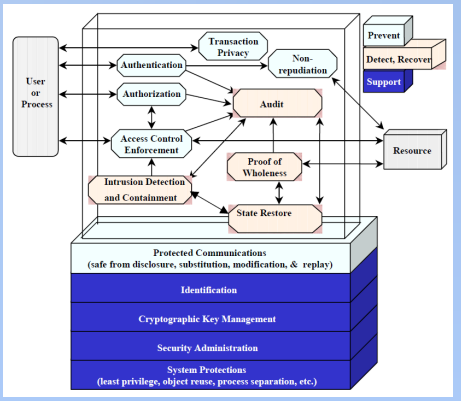
58 CONTROLOS DE SEGURANÇA

- Controlos Tecnológicos
  - de Suporte
  - Preventivos
  - Para detecção e recuperação



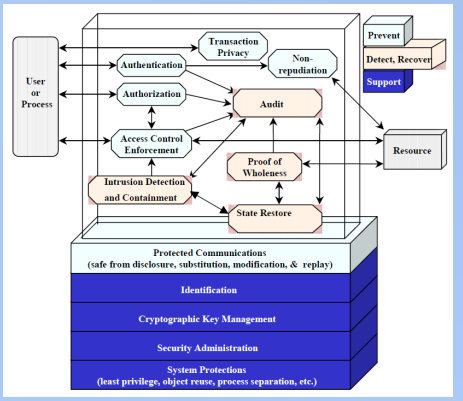
CONTROLOS DE SEGURANÇA

- Controlos Técnicos de Suporte
  - São a base e estão interligados com outros controlos de segurança
  - Identificação
    - Permite a identificação de utilizadores, processos e recursos informacionais
  - Gestão de Chaves Criptográficas
    - Proporcionam uma gestão segura e eficiente
    - das chaves, utilizadas por outros controlos

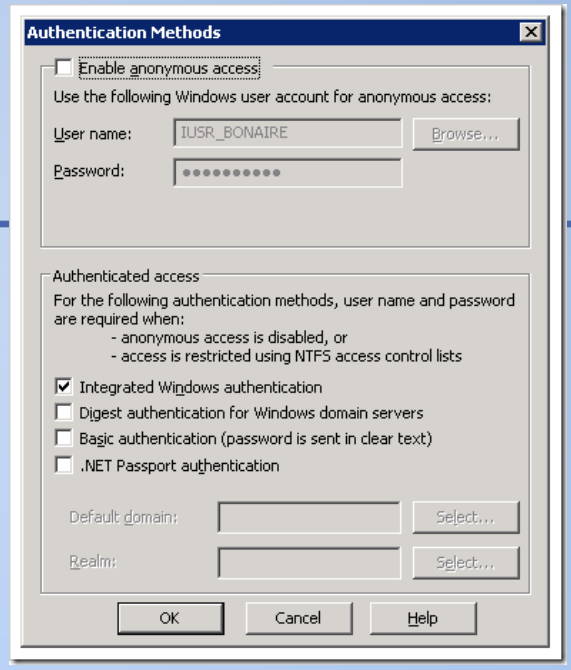


CONTROLOS DE SEGURANÇA

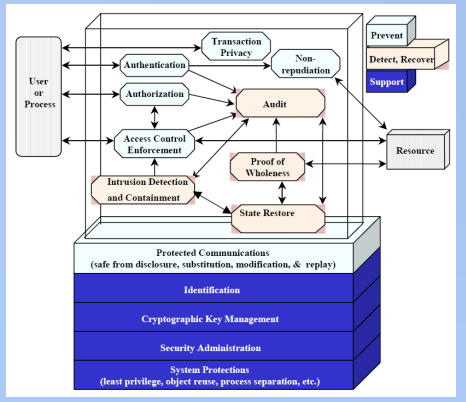
- Controlos Técnicos de Suporte (cont.)
  - Administração da Segurança
    - Configuração apropriada dos sistemas e aplicações tendo em conta as características de cada instalação
    - Ativação ou desativação de registos de auditoria
  - Proteção de Sistemas
    - Em que a segurança é atingida através de uma
    - implementação cuidada de cada sistema
      - Na sua conceção, desenvolvimento e instalação
        - Cuidados na proteção da informação residual (apagar se sensível)
        - A atenção à informação disponibilizada (respeitar a necessidade de conhecer)
        - Separação de processos
        - Modularidade
        - Desenvolvimento por camadas



CONTROLOS DE SEGURANÇA

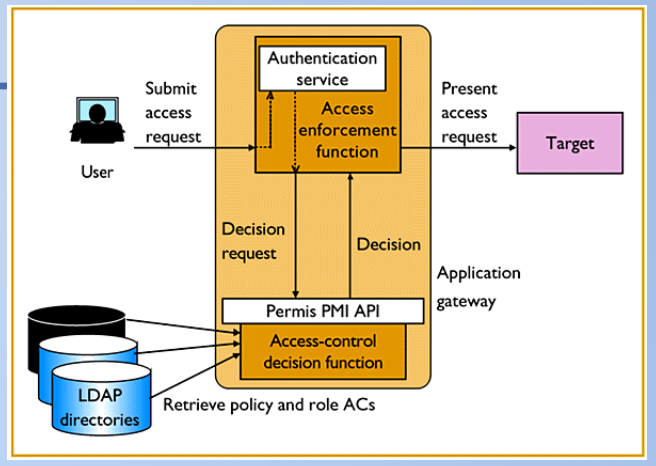


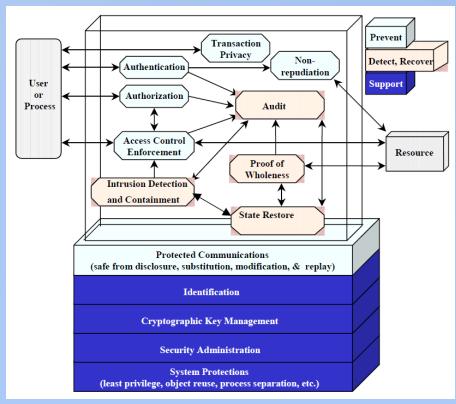
- Controlos Técnicos Preventivos
  - Autenticação
    - Assegura o processo de controlo de
    - identidade
    - Vários mecanismos:
      - User/Pass
      - PIN
      - Autenticação forte
      - Biometria
  - Autorização
    - Permite a especificação e posterior gestão das ações permitidas num determinado sistema
    - Quem ou que objetos podem criar ou apagar ficheiros
    - Quem pode executar determinada aplicação



62 CONTROLOS DE SEGURANÇA

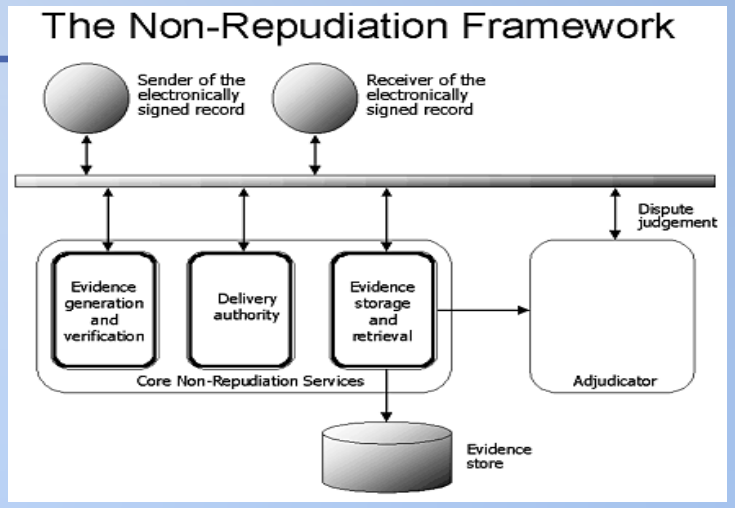
- Controlos Técnicos Preventivos
  - Controlo de Acessos
    - Visa conseguir a Integridade e confidencialidade da Informação, respeitando a política de segurança
  - Algumas técnicas de Controlo de Acesso
    - Attribute-Based Access control (ABAC)
      - Controlo de acessos baseado nos atributos do utilizador
      - Por exemplo: a idade >18, uu local/morada
    - Discretionary Access Control (DAC)
      - Acesso controlado pelo utilizador ou criador do objecto
      - Ex: Permissões de Ficheiros, ACLs (access control lists)
    - Mandatory Access Control (MAC)
      - Controlado pelo sistema. Utilizado para implementar segurança a vários níveis, em informação sensível (tipicamente governo e militares)
      - Ex: sensitivity labels – todos os utilizadores e objectos têm uma label atribuída.
      - Utilizador só tem acesso a certo documento ou funcionalidade se a sua label estiver de acordo com a label do objecto.
    - Role Based Access Control (RBAC)
      - Controlado pelo sistema, mas baseado nas funções atribuídas a utilizadores ou grupos
      - Role assignment: Só pode executar uma transacção de tiver essa função atríbuida
      - Role authorization: dá utorização de determinados utilizadores utilizarem essa função
      - Transaction authorization: em conjunto com 1 e 2 assegura que a transacção só é realizada por utilizadores autorizados

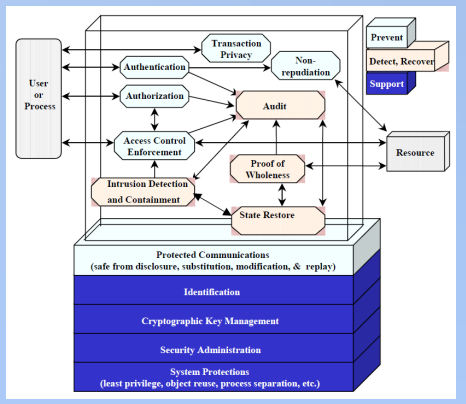




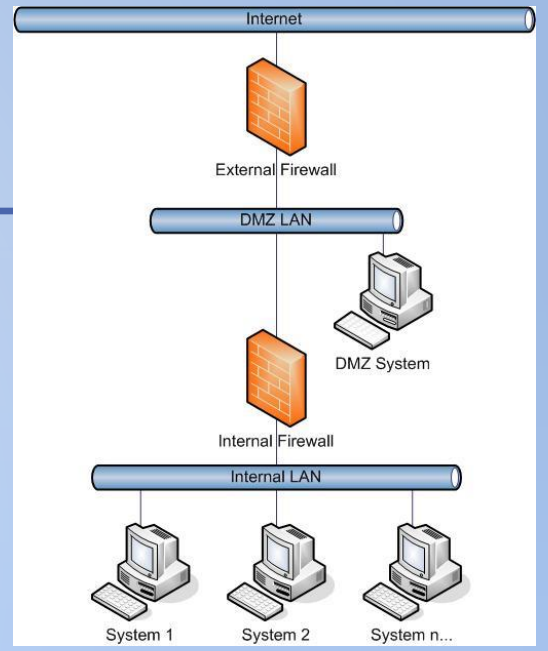
CONTROLOS DE SEGURANÇA

- Controlos Técnicos Preventivos
  - Não repudio
    - Assegurar e garantir a responsabilidade de determinada ação
      - Envio ou receção de documento
      - Criar ou apagar dados
      - …
    - Ao assegurar a correta "accountability"
      - das transações relevantes
      - previne o não repúdio

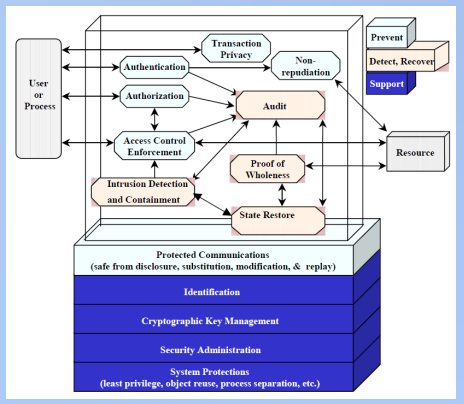




CONTROLOS DE SEGURANÇA

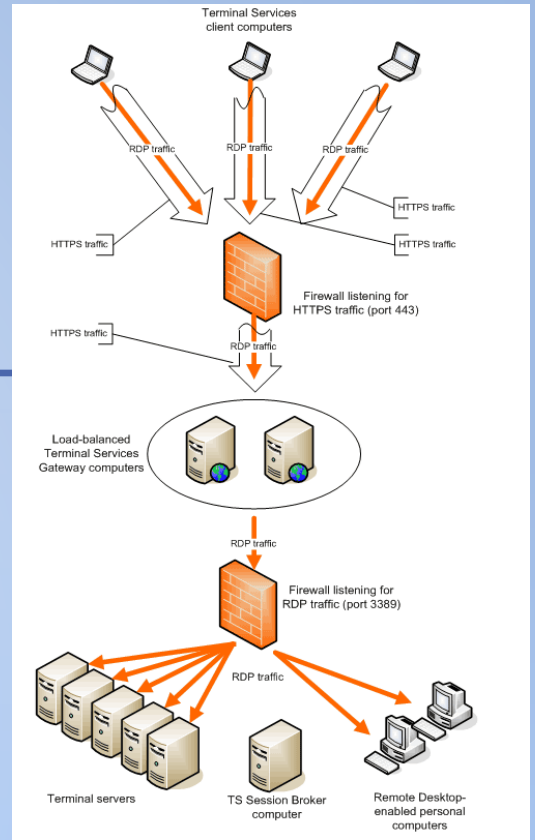


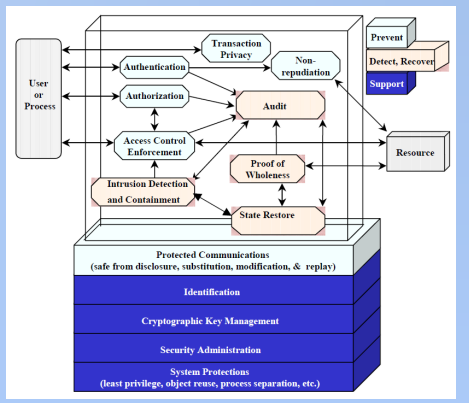
- Controlos Técnicos Preventivos
  - Proteção das comunicações
    - A segurança das comunicações é hoje um requisito para a generalidade das infra-estruturas
    - Assegura a confidencialidade, integridade e disponibilidade
      - Estabelecimento de VPNs, IPSEC, recorrendo a mecanismos criptográficos, para garantir a
      - integridade e confidencialidade
      - Implementação de segurança perimétrica, para manter a disponibilidade – Firewall, IPS(?)
    - Em certos cenários: necessário garantir segurança nas comunicações internas
    - Com especial atenção para a WLAN



CONTROLOS DE SEGURANÇA

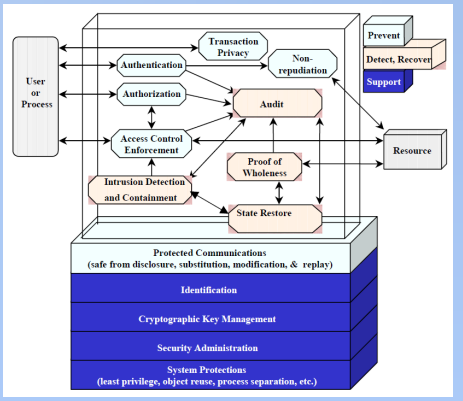
- Controlos Técnicos Preventivos
  - Privacidade das transações
    - Implementação de mecanismos que assegurem a privacidade de determinadas transações
    - Pode ser utilizado o SSL - Secure Sockets Layer
      - Para transferência segura de dados entre serviços como email ou HTTP (neste caso HTTPS)
    - Ou o SSH - Secure Shell
      - para interligação de dois sistemas, permitindo a execução de comandos remotos
    - Não esquecer que a privacidade da transação assegura apenas parte da privacidade de dados ou ações
      - Os dados gravados devem também ser acautelados através de formas de armazenamento dos dados e mecanismos de controlo de acessos





CONTROLOS DE SEGURANÇA

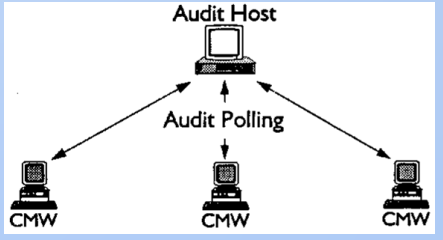
- Controlos Técnicos para deteção e recuperação
  - Controlos que permitem a deteção de violação ou tentativa de violação das regras de políticas
  - Funcionam como complemento à segurança das medidas de suporte e preventivas
  - Controlos:
    - Audit.
    - Intrusion Detection and Containment.
    - Restore Secure State.
    - Virus Detection and Eradication.

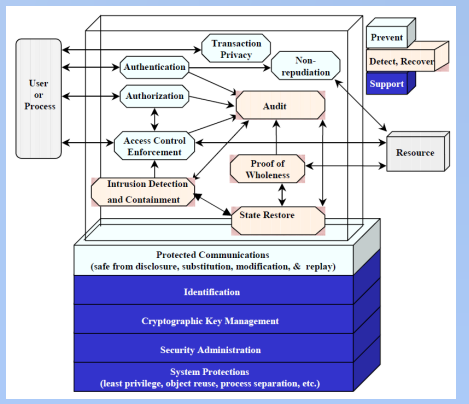


67 CONTROLOS DE SEGURANÇA

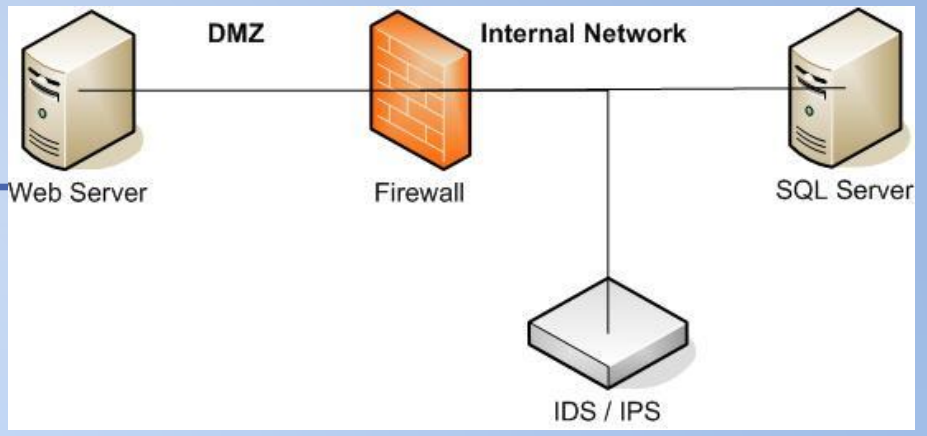
- Controlos Técnicos para deteção e recuperação
  - Audit
    - Análise de registos de auditoria/logs de sistema
    - Deteta eventos/acontecimentos à posteriori
    - Pode conduzir à recuperação de sistemas
    - Vantagem na centralização

      e utilização de aplicação específica

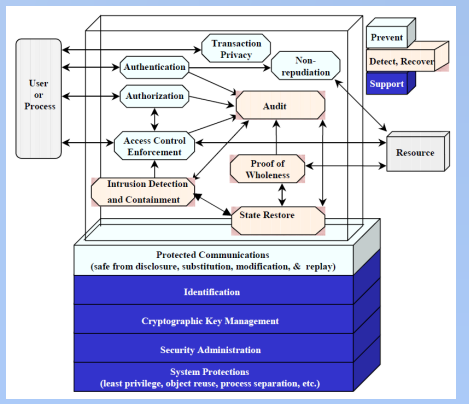




CONTROLOS DE SEGURANÇA

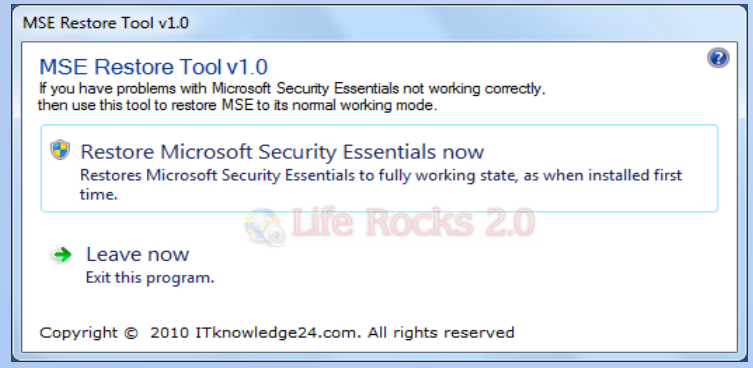


- Controlos Técnicos para deteção e recuperação
  - Intrusion Detection and Containment
    - Utilizado para detetar intrusões ou tentativas de intrusões
    - Pode atuar ativamente para conter a ameaça
    - Ou simplesmente lançar alertas
      - Uma tentativa de intrusão pode não ser concretizada, mas constituir prova
      - Requerer novos controlos
        - atualizações
        - ou configurações

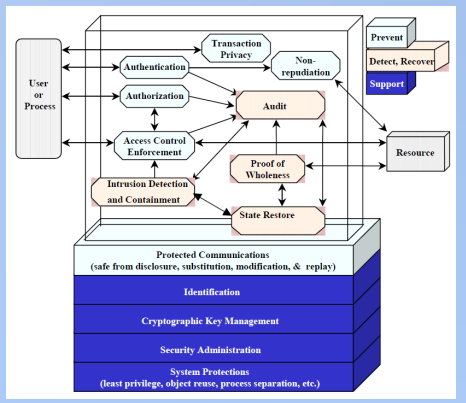


69 CONTROLOS DE SEGURANÇA

- Controlos Técnicos para deteção e recuperação
  - Restore Secure State
    - Permite repor o sistema para um estado seguro
    - Sistemas já disponibilizam ferramentas



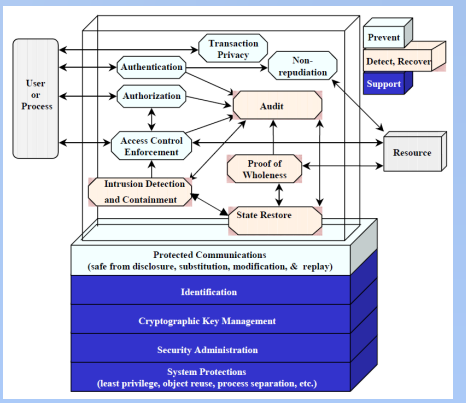
  - Virus Detection and Eradication
    - Deve ser instalado em servidores e postos de trabalho
      - Para detetar, identificar e remover virus



CONTROLOS DE SEGURANÇA

- Objetivos de segurança atingidos com os controlos tecnológicos
  - Assurance: é a garantia ou a confiança dada pela devida implementação das restantes medidas, e correcto funcionamento

Security objectives → Security services ↓	Availability	Integrity	Confidentiality	Accountability	Assurance
Identification					
Cryptographic key management					
Security administration					
System protections					
Protected communications					
Authentication					
Authorization					
Access control enforcement					
Non-repudiation					
Transaction privacy					
Audit					
Intrusion detection and containment					



CONTROLOS DE SEGURANÇA

- Controlos não tecnológicos
  - Devem ser implementados em conjunto com os controlos tecnológicos
  - Contribuindo para gerir e minorar o risco
  - Constituídos por:
    - Controlos de Gestão e Organizacionais
      - Focados na definição de políticas e normas de proteção da informação, realizadas através de procedimentos operacionais
      - Processos e procedimentos que definem como os elementos da organização devem atuar no sentido de colaborar na segurança
    - Controlos Operacionais
      - Conjunto de controlos e linhas orientadoras que assegurem procedimentos seguros de governação do IT, no sentido de cumprir os objetivos da organização

72 CONTROLOS DE SEGURANÇA

- Controlos de Gestão da Segurança
  - Controlos Preventivos
    - Atribuir responsabilidades relativas à segurança dos sistemas críticos
    - Estabelecer e manter planos de segurança de suporte ao IT, que documentem
      - os controlos implementados
      - o plano de implementação de novos controlos
    - Implemente controlos de segurança pessoal
      - Separação de funções
      - Privilégios mínimos
      - Criação e desativação de contas de utilizadores e computadores
      - Registo de utilização
    - Estabeleça programas de formação e sensibilização dos utilizadores
      - Dando a conhecer os cuidados e regras de utilização dos sistemas
      - Responsabilidade de cada um na proteção da informação
    - Estabelecimento de procedimentos para acesso de terceiros
      - parceiros, fornecedores, clientes, prestadores de serviços

CONTROLOS DE SEGURANÇA

- Controlos de Gestão da Segurança
  - De deteção
    - Implementar medidas de segurança de pessoal como
      - Credenciação de pessoal
        - analisando as competências e o passado (p.e. Registo Criminal e Referências)
      - Rotação de funções
    - Conduzir o processo de gestão de risco
    - Conduzir a revisão e atualização dos controlos de segurança
    - Realização de auditorias periódicas
    - Analise e subscreva a aceitação de riscos residuais
  - De recuperação
    - Providenciar o estabelecimento e gestão de um plano operacional de continuidade de negócio
    - Criar capacidade de resposta a incidentes
      - estabelecendo responsabilidades e papeis

74 CONTROLOS DE SEGURANÇA

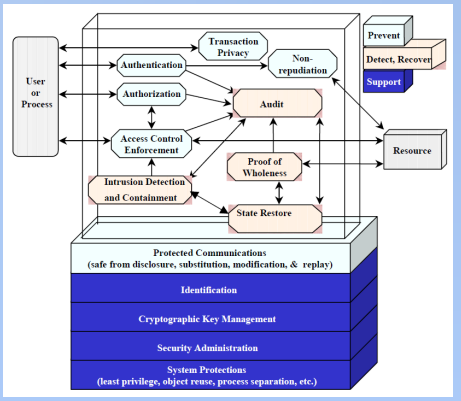
- Controlos Operacionais da Segurança
  - Preventivos
    - Controlar o acesso aos dados e à sua eliminação quando necessário
    - Controlar novos virus de software e a adequação dos controlos implementados (AV)
    - Manter em segurança os sistemas informáticos
      - Proteções de segurança dos equipamentos
      - Garantir os procedimentos definidos para as visitas
      - Manter os sistemas de controlo de acessos, por cartão ou biométricos
    - Manter em segurança os sistemas de rede e cablagem
    - Providenciar os mecanismos adequados de backup
      - Assegurando a salvaguarda de toda a informação necessária à recuperação
    - Estabelecer e controlar os procedimentos de segurança de armazenamento de dados for a da organização
    - Proteger os sistemas contra o fogo
      - Requer manter e conhecer os procedimentos de combate a incêndio
    - Providenciar e assegurar o funcionamento de geradores e UPSs
    - Controlo ambiental do Data Center (Ar condicionado)
      - E outros locais onde estejam equipamentos informáticos ou armazenados os dados

CONTROLOS DE SEGURANÇA

- Controlos Operacionais da Segurança
  - De deteção
    - Providenciar a segurança física (deteção de intrusões, alarmes, CCTV)
    - Assegurar a segurança ambiental (detetores de incêndios, sensores de temperatura e humidade, e alarmes).

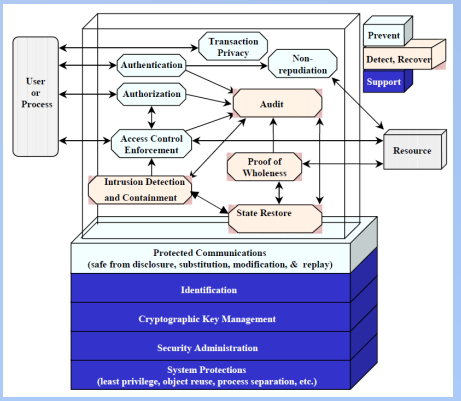
CONTROLOS DE SEGURANÇA

- Exercício – Identificar controlos de segurança
  - Controlos não tecnológicos
    - Controlos de Gestão e Organizacionais
      - Preventivos
      - de Deteção
      - de Recuperação
    - Controlos Operacionais
      - Preventivos
      - de Deteção



77 CONTROLOS DE SEGURANÇA

- Exercício – Identificar controlos de segurança
  - Controlos Técnicos de Suporte
    - Identificação
    - Gestão de Chaves Criptográficas
    - Administração da Segurança
    - Proteção de Sistemas
  - Controlos Técnicos Preventivos
    - Autenticação
    - Autorização
    - Controlo de Acessos
    - Não repudio
    - Proteção das comunicações
    - Privacidade das transações
  - Controlos Técnicos para deteção e recuperação
    - Audit.
    - Intrusion Detection and Containment.
    - Proof of Wholeness.
    - Restore Secure State.
    - Virus Detection and Eradication.



AGENDA

- Introdução à Gestão de Continuidade de Negócio
- A avaliação e gestão de riscos
- Tratamento dos Riscos
- Controlos de segurança
  - Tecnológicos, Operacionais e de Gestão

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

SEGURANÇA DA INFORMAÇÃO

E NORMAS APLICÁVEIS

LUIS AMORIM

26 Mar 2022