Segurança e Gestão de Risco

2ºSem 2023/24

O Processo FRAAP

LUIS AMORIM

23 Mar 2024

Síntese da Aula Anterior

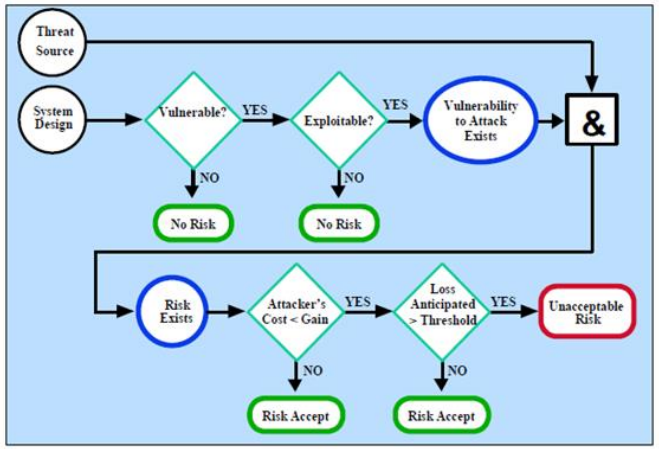
- Tratamento dos Riscos

- Controlos de segurança
  - Tecnológicos, Operacionais e de Gestão

- Modelo de segurança integrado
  - Controlos de segurança alinhados com as melhores práticas

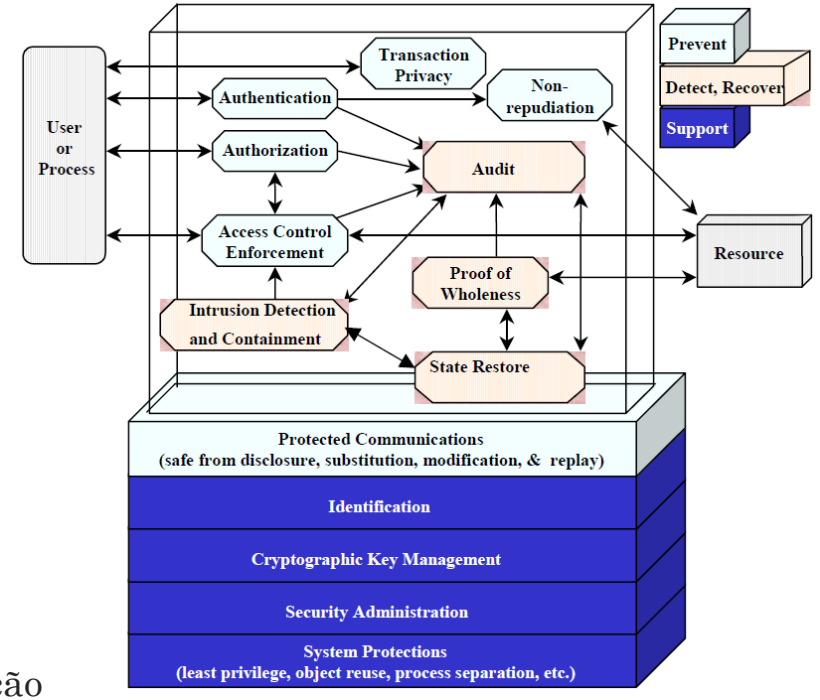
Síntese

- Tratamento dos Riscos
  - Opções de Mitigação de Risco
    - Administrativas
      - Assumir o Risco, Evitar o Risco, Transferência de Risco, Planeamento de R
    - Predominantemente técnicas:
      - Limitar o Risco, Reconhecimento e Desenvolvimento de controlos
    - Fluxo de aceitação de riscos Ou não aceitação e implementação de controlos
    - Análise de opções de mitigação utilizando o Risk Mitigation Checklist (estraído do NIST)
    - Passos para a implementação de controlos
    - Ter em atenção que a implementação de controlos pode gerar novas vulnerabilidades



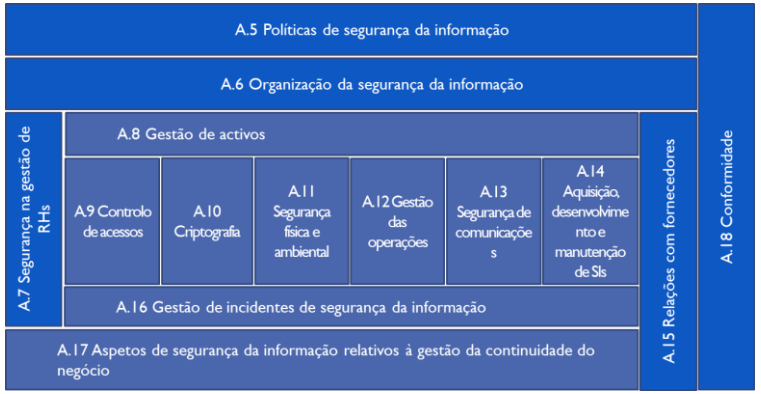
Síntese

- Controlos de segurança
  - Tecnológicos
    - de Suporte
    - Preventivos
    - Para detecção e recuperação
  - Não tecnológicos:
    - Controlos de Gestão e Organizacionais
      - definição de políticas e normas de protecção da informação
      - definem como os elementos da organização devem actuar
    - Controlos Operacionais
      - controlos e linhas orientadoras que assegurem procedimentos seguros
      - considerando as políticas e normas definidas na gestão



Síntese Abordagem Integrada à Segurança

- Abordagem Integrada à Segurança
  - A Segurança de um Sistema de Informação requer uma abordagem holística e integrada:
    - Normas e Procedimentos
    - Sistemas e Aplicações
    - Infra-estrutura
    - Acesso Físico
  - Com medidas de segurança Tecnológicas e administrativas/operacionais
    - Conforme espelhado nas melhores práticas (p.e. ISO 27002)



Exemplos de ameaças

- Coloquem-se no lugar do Responsável de Segurança da Prisão
  - O que falhou?
  - Ameaça? → Impersonificação
  - Vulnerabilidades?
  - Que controlos implementarias?

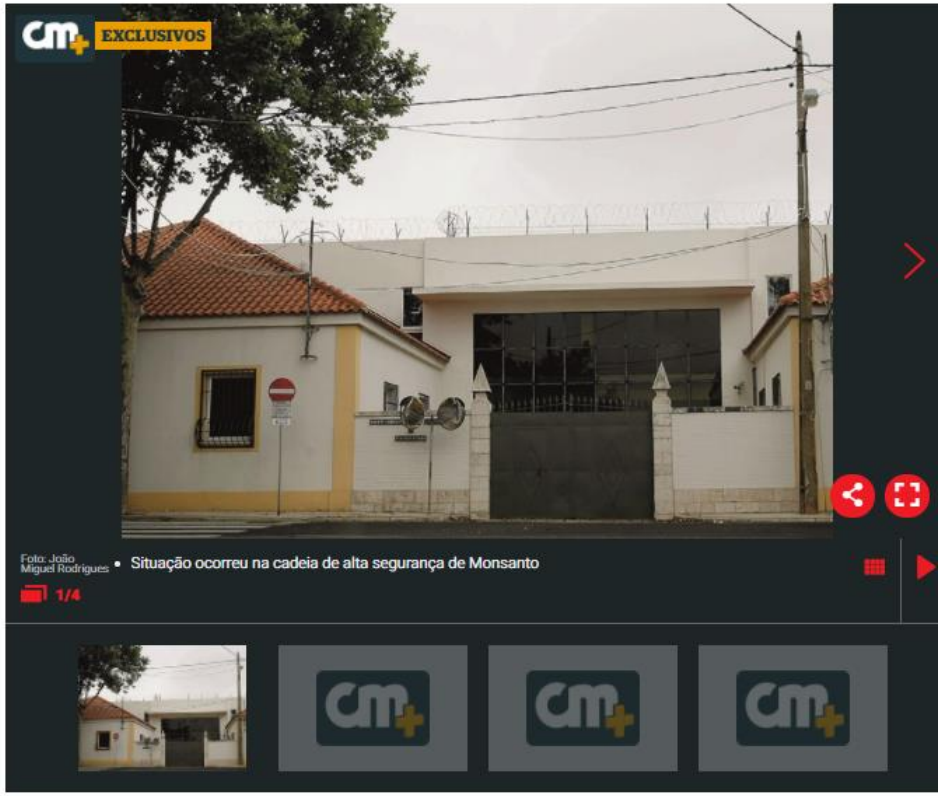
procedimento

criar um procedimento e sensibilizar.

Entra em prisão de alta segurança com emails

Mulher mostra alegada troca de correspondência com diretora-adjunta do estabelecimento prisional e consegue visitar um dos 21 refugiados marroquinos ali retidos.

Miguel Curado | 11 de Outubro de 2020 às 01:30



EXCLUSIVOS precisou apenas de mostrar alguns emails que disse ter trocado com a diretora-adjunta da cadeia de alta segurança de Monsanto, em Lisboa, para conseguir entrar na mesma e visitar um dos 21 refugiados marroquinos que ali se encontram há várias semanas, à espera de decisão do respetivo processo de extradição.

Exemplos de ameaças

- Coloquem-se no lugar do Responsável de Segurança da Elétrica
  - O que falhou?
  - Ameaça?
  - Vulnerabilidades?
  - Que controlos implementarias?

Phishing 4+3

Social Engineering 2+4

Hacking 3+4

Jamming 1+2

Sensibilização e protocolos.

Mais ...

Como a energia elétrica se tornou o novo campo de batalha entre EUA e Rússia

Lioman Lima - @liomanlima
BBC News Mundo

19 junho 2019

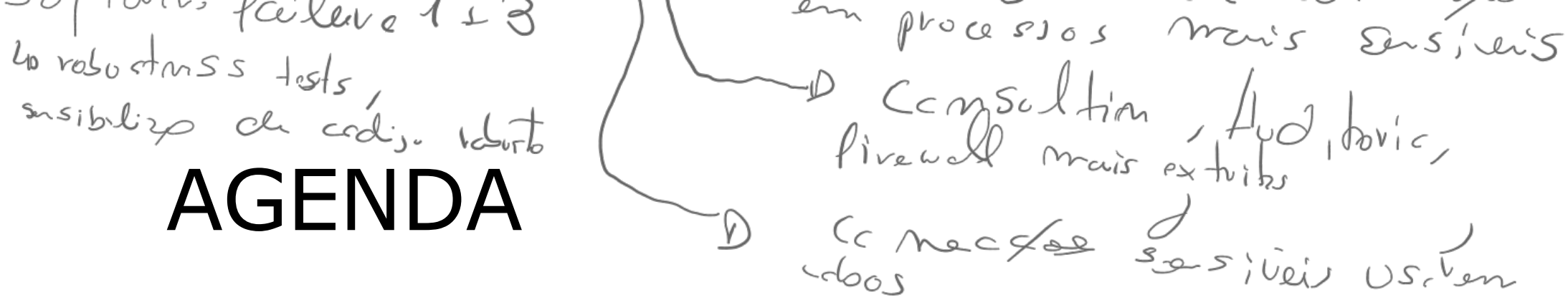
Redes elétricas e outras estruturas vitais estão na mira das tensões entre a Rússia e os Estados Unidos

Em 23 de dezembro de 2015, uma parte da Ucrânia ficou às escuras.

Foi uma noite dentro da noite: ninguém sabia ao certo o que tinha acontecido.

As usinas não haviam registrado nenhuma falha, os geradores funcionavam normalmente, tudo parecia correr dentro dos parâmetros.

Até que cerca de 700 mil pessoas ficaram sem eletricidade.



AGENDA

- **O processo de análise de risco FRAAP**
  - Introdução
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP
  - Ferramentas de apoio ao processo

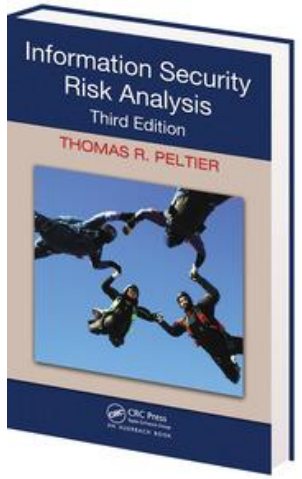
- Identificação de ameaças e controlos para
  - a Cibersegurança
  - a Privacidade
  - Serviços na Cloud

Exercício de Grupo

- Conduzir uma Avaliação dos Riscos

Processo de análise de Risco FRAAP

- Facilitated Risk Analysis and Assessment Process
  - É uma metodologia de análise e avaliação de risco desenvolvido por Thomas R. Peltier
    - Tem por base as normas existentes (nomeadamente a 17799/27002)
      - Que transmitem as boas práticas, não a metodologia
    - Resulta da experiência da equipa em projectos
    - Tem sido utilizada, e melhorada, nos últimos15 anos
    - Prima por:
      - Ser dirigido pelo responsável de negócio
      - Levar dias, em vez de semanas
      - Boa relação custo-benefício
      - Utilizar especialistas/experiencia interna

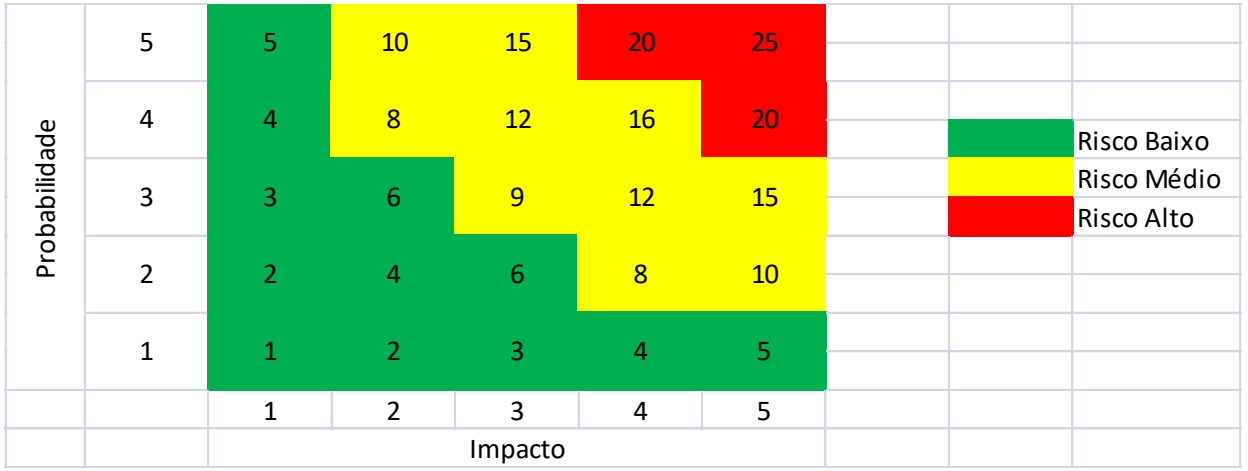


Processo de análise de Risco FRAAP

- Facilitated Risk Analysis and Assessment Process
  - Este processo envolve a análise de 1 sistema, plataforma, processo de negócio de cada vez
  - A afinação do processo, baseada na experiência prática, torna-se
    - Rápido
    - Fácil de implementar
    - Envolve a organização

Processo de análise de Risco FRAAP

- Facilitated Risk Analysis and Assessment Process
  - Autor defende a utilização de um método qualitativo
    - Em detrimento de métodos quantitativos
    - A utilização de valores no cálculo resulta num valor final difícil de interpretar
    - Podem ser definidos níveis para medição, mas a interpretação ser qualitativa



Processo de análise de Risco FRAAP

- Método Qualitativo vs Quantitativo

Quantitative Risk Assessment	*Qualitative Risk Assessment*
Advantages	**Advantages**
The results are based substantially on independently objective processes and metrics.	Calculations are simple.
Great effort is put into asset value definition and risk mitigation.	It is not necessary to determine monetary value of asset.
Cost–benefit assessment effort is essential.	It is not necessary to quantify threat frequency.
Results can be expressed in management-specific language.	It is easier to involve nonsecurity and nontechnical staff.
	It provides flexibility in process and reporting.

Processo de análise de Risco FRAAP

- Método Quantitativo vs Qualitativo

Quantitative Risk Assessment	*Qualitative Risk Assessment*
Disadvantages	**Disadvantages**
Calculations are complex.	It is very subjective in nature.
Historically, it only works well with a recognized automated tool and associated knowledge base.	Limited effort is required to develop monetary value for targeted assets.
There is a large amount of preliminary work.	There is no basis for the cost–benefit analysis of risk mitigation.
It is not presented on a personnel level.	
Participants cannot be coached easily through the process.	
It is difficult to change directions.	
It is difficult to address out-of-scope issues.	

Processo de análise de Risco FRAAP

- Avaliação qualitativa vs Avaliação quantitativa (visto anteriormente)

> "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.

Processo de análise de Risco FRAAP

- Facilitated Risk Analysis and Assessment Process
  - Durante o processo a equipa envolvida é conduzida a participar na discussão e identificação de
    - potenciais ameaças
    - níveis de risco
    - possíveis controlos a aplicar

Processo de análise de Risco FRAAP

- Vantagens do FRAAP
  - É realizado em alguns dias, em vez de semanas/meses
  - Envolve o responsável de negócio
    - Participa no processo
    - Compreende as necessidades de implementação
    - Envolvido na selecção de controlos eficientes (custo-benefício)
  - Envolve as áreas de negócio
    - Reconhecimento da participação e controlo do processo
  - Permite à equipa participar na selecção de controlos apropriados
  - Facilita a Gestão da Mudança

Processo de análise de Risco FRAAP

- Equipa envolvida
  - Responsável de negócio do processo, sistema ou activo
  - Gestor de Projecto - nomeado pelo gestor de negócio
    - O seu papel é acompanhar o desenrolar do projecto e garantir as condições necessárias requeridas pela equipa (sala, agendar reunião…)
  - Facilitador → exterior
    - consultor com conhecimento do FRAAP
  - Escriba ou secretário(a)
    - responsável por documentar as reuniões
  - Especialistas relacionados com o objecto
    - Negócio
    - IT
    - Users

Processo de análise de Risco FRAAP

- Facilitador
  - Consultor que ajude a conduzir o grupo no sentido de obter os resultados esperados
    - Ameaças, probabilidades, impacto, nível de risco
  - Guiar a equipa pelas várias áreas de interesse
    - Identificando o maior número de ameaças
  - Manter o grupo focado no tema
  - Actuar como regulador e árbitro da sessão
  - Controlar o tempo

Processo de análise de Risco FRAAP

- Facilitador
  - Deve observar as seguintes regras
    - Encorajar a participação de todos
    - Aceitar todas as sugestões
    - Envolver os participantes, escutando opiniões
    - Estar atento às movimentações, gestos, silêncios
    - Actuar como regulador e árbitro da sessão
    - Deve ser imparcial, sem tomar posições particulares, mas guiando a equipa quando está perdida ou é preciso consenso
    - Ser objectivo

Processo de análise de Risco FRAAP

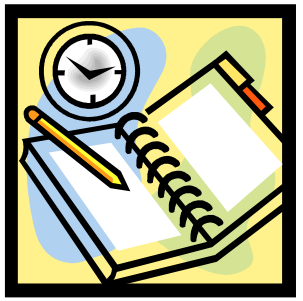
- Escriba ou secretário(a)
  - Responsável por documentar as reuniões
  - Assegura que todas as ameaças, controlos e acções são registadas
  - Libertando o facilitador desta função, permite-lhe desempenhar melhor a sua função principal

Processo de análise de Risco FRAAP

- Especialistas relacionados com o objeto em análise
  - São elementos da própria organização que conhecem o sistema ou processo em análise
  - Deve ser uma equipa equilibrada, entre as várias áreas de competência
    - Conhecimento do negócio, familiarizados com a missão do objecto em análise
    - Utilizadores que conheçam as vulnerabilidades e ameaças
    - Técnicos IT com conhecimento da infra-estrutura e sistemas em causa
  - Elementos devem conseguir funcionar em equipa

Processo de análise de Risco FRAAP

- Facilitated Risk Analysis and Assessment Process
  - Este processo envolve a análise de 1 sistema processo, plataforma, processo de negócio definido de cada vez
  - Pre-FRAAP
    - Reunião de 1 a 1,5 horas como responsável de negócio
    - Vão definir as bases de trabalho para as fases seguintes
  - FRAAP
    - Dura aproximadamente 4 horas e deve incluir uma equipa mais abrangente que inclua os responsáveis de negócio e da infra-estrutura
    - Identificar: Ameaças, Vulnerabilidades, Impactos e Controlos
  - Post-FRAAP
    - Normalmente 1 a 2 semanas
    - Análise dos resultados e produção do relatório final



Processo de análise de Risco FRAAP

- Antes de iniciar deve existir um Programa de Sensibilização
  - Dar a conhecer o processo
  - Envolver os participantes
  - Este Programa deve ser conduzido de forma a
    - Avaliar o conhecimento relativo a avaliação de risco
    - Determinar o que os gestores e outros funcionários pretendem aprender
    - Verificar o nível de aceitação do programa de segurança
    - Traçar forma de conquistar a aceitação
    - Identificar possíveis aliados

Processo de análise de Risco FRAAP

- Ferramentas para um Programa de Sensibilização?
  - eMail
  - Site
  - Cartazes
  - Questionários
    - Mail
    - Electrónicos
    - Papel
  - Sessão de apresentação

Processo de análise de Risco FRAAP

- Programa de Sensibilização deve
  - Ser adaptado à organização
    - Ferramentas e linguagem
  - Seleccionar as ferramentas adequadas a cada grupo
  - Encontrar áreas não conformes
    - Trabalhar no sentido de reduzir exposição
      - E resolver possíveis atritos
    - Sem comprometer resultados da avaliação
  - Envolver os utilizadores

Processo de análise de Risco FRAAP

- Pontos chave
  - Garantir o envolvimento dos participantes
  - O processo é da organização, não é do consultor/facilitador
    - Não utilizar expressões como o meu projecto
    - É o Vosso ou Nosso projecto

Processo de análise de Risco FRAAP

- Conceitos chave – funções
  - Owner
    - Deve ser o mais alto responsável da unidade onde o objecto do processo pertence
    - É responsável por:
      - Estabelecer a classificação da informação
      - Identificar controlos razoáveis e prudentes
      - Monitorizar a adequação de implementação de controlos
      - Autorizar o acesso a quem necessita
        - Ou inibição
  - Custodian (IT)
    - Nomeado pelo owner como responsável do controlo
  - User
    - Empregados autorizados a aceder à informação

Sessão Pre-FRAAP

- Reunião de Pre-FRAAP
  - Reunião de 1 a 1,5 horas com o responsável de negócio
  - Deve incluir
    - Gestor de Negócio/Processo e Gestor de Projecto
    - Facilitador
    - Escriba

Sessão Pre-FRAAP

- Resultados esperados
  1. Pré-triagem → Excluir o que não cumpre grande risco
  2. Definição do âmbito
  3. Diagrama com a descrição/detalhe do sistema ou processo a avaliar
  4. Estabelecimento da equipa a incluir no processo
  5. Requisitos para a reunião FRAAP
  6. Acordar definições de principio → termos tem de ser clarificados
  7. Mini-Brainstorming

Sessão Pre-FRAAP

- Resultados do Pre-FRAAP
  - Pré-triagem
    - Utilizar um elemento de avaliação ou a conjugação de vários
    - Escolha dos elementos depende dos propósitos do objecto em análise
    - A conjugação dos elementos determina a necessidade ou não de uma Avaliação de Risco

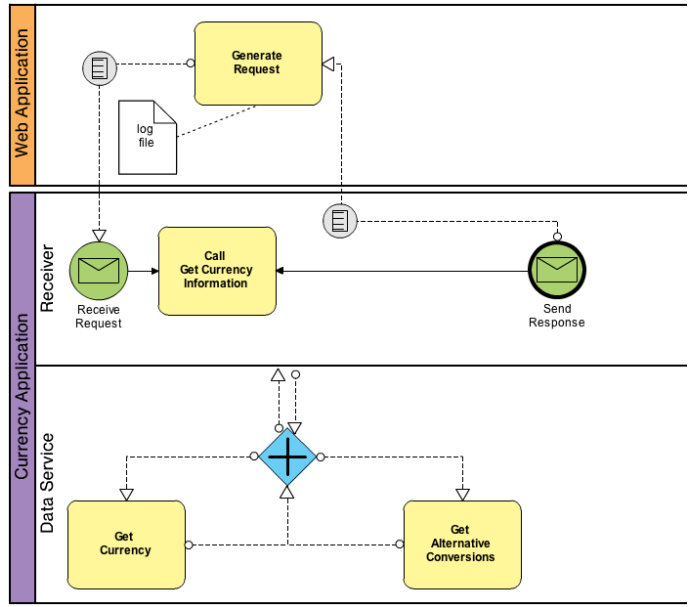
Impacto / Sensibilidade	Alto	Médio	Baixo
Alto	Avaliação Risco	Avaliação Risco	Avaliação Risco
Médio	Avaliação Risco	Avaliação Risco	Implementar Controlos base
Baixo	Avaliação Risco	Implementar Controlos base	n.a.

Sessão Pre-FRAAP

- Resultados do Pre-FRAAP
  - Definição do âmbito
    - Qual o âmbito da avaliação a realizar
  - Identificar categorias de ameaças
    - Tendo como base a C-I-A
    - Mas podendo incluir outras como a performance ou reliability

Sessão Pre-FRAAP

- Resultados do Pre-FRAAP
  - Diagrama com a descrição/detalhe do sistema ou processo a avaliar
    - Diagrama com a descrição do processo em análise
    - Para documentação e informação da equipa FRAAP
    - “uma imagem vale por mil palavras”
  - Estabelecimento da equipa a incluir no processo
    - Identificar entre 15 a 30 elementos



Sessão Pre-FRAAP

- Resultados do Pre-FRAAP
  - Requisitos para a reunião FRAAP
    - Agendamento
    - Sala
    - Materiais …
  - Acordar definições de principio
    - O que é Activo, Ameaça, Vulnerabilidades, Probabilidade, Impacto, Risco, …

Activo	É um recurso com valor. Pode ser uma pessoa, um processo, informação, …
Ameaça	É qualquer coisa (acto humano intencional ou não, ou causada pela natureza), que tem o potencial de causar danos
Probabilidade	Quantificação da possibilidade uma dada ameaça acontecer
Impacto	O efeito de uma ameaça sobre um activo, expresso em termos tangíveis ou intangíveis
Vulnerabilidades	É uma fragilidade que pode ser usada para colocar em perigo ou causar danos a um activo de informação
Riscos	Risco é a combinação de ameaça com probabilidade e impacto, expresso em níveis de valor acordados

Sessão Pre-FRAAP

- Resultados do Pre-FRAAP
  - Mini-Brainstorming
    - No sentido de identificar algumas ameaças como introdução à reunião FRAAP

Confidencialidade	Integridade	Disponibilidade
Dados de cliente podem ser interceptados	Dados podem ser introduzidos (inadvertidamente) incorretamente	Ficheiros guardados em pastas pessoais podem não estar disponíveis
Roubo interno de informação	Programa com falhas pode alterar dados	Falhas de hardware podem ter impacto na disponibilidade servers
Documento papel ou electrónicos podem chegar a pessoas não autorizadas	Introdução intencional de dados errados	Falha no circuito de dados pode impedir acesso a sistema
Informação confidencial deixada à vista na secretária	Falha na reposição de backup	Catástrofes ambientais
Conversas fora do escritório podem divulgar informação sensível	Upgrade de software corrompe base de dados	Upgrades de software podem impedir acesso

Sessão Pre-FRAAP

- Checklist

para reunião

- Garantir abordagem de todos os pontos

ISSUE	REMARKS
PRIOR TO THE MEETING	
1. Date of Pre-FRAAP Meeting *Record when and where the meeting is scheduled*	
2. Project Executive Sponsor or Owner *Identify the owner or sponsor who has executive responsibility for the project*	
3. Project Leader *Identify the individual who is the primary point of contact for the project or asset under review*	
4. Pre-FRAAP Meeting Objective *Identify what you hope to gain from the meeting – typically the seven deliverables will be discussed*	
5. Project Overview *Prepare a project overview for presentation to the pre-FRAAP members during the meeting*	
Your understanding of the project scope	
The FRAAP methodology	
Milestones	
Pre-screening methodology	
6. Assumptions *Identify assumptions used in developing the approach to performing the FRAAP project*	
7. Pre-screening Results *Record the results of the pre-screening process*	

Sessão Pre-FRAAP

- Checklist

  para reunião

DURING THE MEETING	
8. Business Strategy, Goals and Objectives *Identify what the owner's objectives are and how they relate to larger company objectives*	
9. Project Scope *Define specifically the scope of the project and document it during the meeting so that all participating will know and agree*	
• **Applications/Systems**	
• **Business Processes**	
• **Business Functions**	
• **People and Organizations**	
• **Locations/Facilities**	
10. Time Dependencies *Identify time limitations and considerations the client may have*	
11. Risks/Constraints *Identify risks and/or constraints that could affect the successful conclusion of the project*	
12. Budget Identify any open budget/funding issues	
13. FRAAP Participants *Identify by name and position the individuals whose participation in the FRAAP session is required*	
14. Administrative Requirements *Identify facility and/or equipment needs to perform the FRAAP session*	
15. Documentation *Identify what documentation is required to prepare for the FRAAP session (provide the client the FRAAP Document Checklist)*	

AGENDA

- Revisão da sessão anterior
  - O Processo FRAAP - Facilitated Risk Analysis and Assessment Process

- O processo de análise de risco FRAAP
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP
  - Ferramentas de apoio ao processo
  - Exercício Prático

Sessão FRAAP

- Sessão de trabalho
  - Não deve durar mais que quatro horas
    - É suficiente, na maioria dos casos
    - Difícil arranjar mais disponibilidade
  - Envolver todos os elementos da equipa
    - Identificados no Pre-FRAAP
    - E devidamente convocados

Sessão FRAAP

- FRAAP
  - Resultados esperados
    - Identificação das Ameaças
    - Identificação das Vulnerabilidades
    - Identificação dos Controlos Existentes
    - Calculo dos Riscos
    - Identificação de novos controlos
    - Caracterização dos Riscos Residuais

= o Risco Inerente

Sessão FRAAP

- Sessão de trabalho
  - Requisitos da reunião
    - Assegurar materiais necessários
      - Projector
      - Quadro
      - Canetas
    - Disposição da Sala em U
      - Importante para assegurar a participação de todos
      - Todos estão na linha da frente, com o facilitador
    - Desencorajar a utilização de portáteis ou PDAs
    - Lembrar para desligar os telemóveis
      - Ou colocar em silêncio

Sessão FRAAP

- Agenda

FRAP Session Agenda	Responsibility
• Introduction	
• Explain the FRAP process and cover definitions	• Owner + Facilitator
• Review scope statement	• Owner
• Review Visual Diagram	• Technical support
• Discuss definitions	• Facilitator

• Review Objectives
  • Identify Threats
  • Establish Risk Levels
  • Identify possible safeguards	

• Identify roles and introduction	• Team
• Review session agreements	
• Brainstorm for threats	• Team
• Establish risk levels (probability and impact)	• Team
• Prioritize threats	• Team
• Identify possible safeguards	• Team
• Create Management Summary Report	• Facilitator

Sessão FRAAP

- Sessão de trabalho - Introdução
  - Explain the FRAP process and cover definitions
    - Responsável de negócio irá
      - Abrir a sessão
      - Introduzir o facilitador
    - Facilitador deverá
      - Apresentar a agenda
      - Explicar o processo
  - Review scope statement - Owner
    - Importante identificar
      - O que foi assumido
      - Constrangimentos identificados
    - Deve ser entregue uma cópia do Scope Statment à equipa

Sessão FRAAP

- Sessão de trabalho - Introdução
  - Review Visual Diagram – Technical support
    - Deve fazer a apresentação do diagrama, explicando o processo
    - Cerca de 5 min.
  - Discuss definitions - Facilitator
    - Apresenta as definições acordadas
    - Se o processo já é conhecido na organização, estas definições já devem estar interiorizadas

Activo	É um recurso com valor. Pode ser uma pessoa, um processo, informação, …
Ameaça	É qualquer coisa (acto humano intencional ou não, ou causada pela natureza), que tem o potencial de causar danos
Probabilidade	Quantificação da possibilidade uma dada ameaça acontecer
Impacto	O efeito de uma ameaça sobre um activo, expresso em termos tangíveis ou intangíveis
Vulnerabilidades	É uma fragilidade que pode ser usada para colocar em perigo ou causar danos a um activo de informação
Riscos	Risco é a combinação de ameaça com probabilidade e impacto, expresso em níveis de valor acordados

Sessão FRAAP

- Sessão de trabalho - Introdução
  - Review Objectives - Facilitator
    - São revistos os objectivos a atingir
      - Identificar ameaças
      - Estabelecer níveis de risco
      - Identificar controlos
    - Serve como introdução à segunda parte da sessão

Sessão FRAAP

- Sessão de trabalho - Introdução
  - Identify roles and introduction - team
    - Os elementos da equipa identificam-se
      - Nome
      - Departamento
      - Localização
      - Contacto

Sessão FRAAP

- Sessão de trabalho - Introdução
  - Review session agreements
    - Todos os elementos devem participar
    - Devem cingir-se aos seus papeis
    - Focar-se no ponto da agenda
    - Todas as ideias têm um valor igual
    - Escutar os outros pontos de vista
    - Todas as questões/contributos serão registados
    - Mesmo os que forem preteridos
    - Colocar e registar a ideia, antes de discuti-la
    - Assegurar que o escriba assenta todas as questões
    - Uma temática (C-I-D) de cada vez
    - Limite de tempo por ativo/atividade (3 a 5 minutos)

Sessão FRAAP

- Condução da reunião
  - Idealmente deve ser respeitada a disposição em U
  - O facilitador deve começar por colocar o primeiro atributo em discussão, colocando os resultados do mini-brainstorming

Confidencialidade **assegurar que a informação não é acedida ou divulgada a pessoas que não devem ter acesso**
Dados de cliente podem ser interceptados
Roubo interno de informação
Documento papel ou electrónicos podem chegar a pessoas não autorizadas
Informação confidencial deixada à vista na secretária
Conversas fora do escritório podem divulgar informação sensível

Sessão FRAAP

- Condução da reunião
  - Solicitar a participação de todos na identificação de ameaças
    - Dar 3 a 5 minutos para pensar em possíveis ameaças
    - Começar numa ponta
    - Percorrer todos
    - Cada elemento só sugere 1 ameaça de cada vez
    - Dar várias voltas até que se esgotem as sugestões
    - Ter em atenção
      - Os manipuladores
      - Centrar no tópico em discussão

Sessão FRAAP

- Condução da reunião
  - Passar ao segundo atributo
    - Começar na outra ponta
    - Utilizar cores diferentes
    - Ir colocando anotações à volta da sala

Integridade **Assegurar a precisão, consistência e confiabilidade da informação**
Dados podem ser introduzidos (inadvertidamente) incorretamente
Programa com falhas pode alterar dados
Introdução intencional de dados errados
Falha na reposição de backup
Upgrade de software corrompe base de dados

Sessão FRAAP

- Utilização de Checklists
  - Para ameaças
  - Para controlos
  - Permite reduzir o tempo de identificação
  - Complementa a identificação feita pelos elementos da equipa

Sessão FRAAP

- Threats Checklists
  - consultar ISO 27005
  - Ou/e Appendix G
    - Table G.1 Sample Threat Checklist
    - Table G.2 Natural Threat List

Threat	Applicable Yes/No
Integrity	
Data stream could be intercepted.	
Faulty programming could (inadvertently) modify data.	
Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons.	
Data could be entered incorrectly.	
Intentional incorrect data entry.	
Use of outdated programs could compromise integrity of information.	
Faulty hardware could result in inaccurate data entry and analysis.	
Third parties could modify data.	
Files could be accidentally deleted.	
Hackers could change data.	
Internal Users could launch unauthorized programs to access and or modify bank data.	
Reports could be falsified	
Internal theft of information by employees could be modified and used later.	
Network sniffing could intercept user passwords and allow unauthorized modification of information	
Information could be outdated.	
Hackers could obtain unauthorized access into network to corrupt system resources.	
Physical intrusion by unauthorized persons.	
Documents could be falsified to appear as official company documents.	
Unauthorized or fictitious sales could be approved.	
Information could be misinterpreted due to language barriers.	
Fraudulent programming could impact data integrity, example: hidden hooks.	
Computer viruses could modify data.	
Information could be misdirected.	
Transactions could be intentionally not run or misrouted.	
Newer or upgraded software could cause corruption of documents or files.	
Non-standard procedures could cause misinterpretation of information.	
Unauthorized persons may use an unattended workstation.	
Information to and from 3rd parties could be corrupted in transmission.	
Account Information may be shared.	
A power failure could corrupt information.	
Information could be submitted in a vague or misleading manner.	
Someone could impersonate a customer to corrupt records (identity theft).	
Information could be taken outside the company	
Integrity of information could be compromised due to decay of information	

Sessão FRAAP

- Threats Checklists
  - Table G.1 Sample Threat Checklist

Threat
Human - Accidental
Fire: Internal-major
Fire: Internal-Catastrophic
Fire: External
Accidental explosion – on site
Accidental explosion – off site
Aircraft crash
Train crash
Derailment
Auto/Truck crash at site
Fire: Internal-minor
Human error – maintenance
Human error – operational
Human error – Programming
Human error – users
Toxic contamination
Medical emergency
Loss of key staff

Threat
Human - Deliberate
Sabotage/Terrorism: External - Physical
Sabotage/Terrorism: Internal - Physical
Terrorism: Biological
Terrorism: Chemical
Bombing
Bomb Threat
Arson
Hostage taking
Vandalism
Labor dispute/Strike
Riot/Civil disorder
Toxic contamination

Sessão FRAAP

- Antes do próximo ponto, fazer pausa
  - Dá oportunidade para
    - Verificar mensagens
    - Tomar um café
    - Limpar

Sessão FRAAP

- Identificação de Controlos existentes
  - Rever todas as ameaças identificando os controlos existentes
  - Esta caracterização permite à equipa identificar melhor o risco actual
  - Razão pela qual é fundamental ter elementos da infra-estrutura
    - Conhecem os controlos actuais

Threat	*Existing Control*
Confidentiality	
Insecure e-mail could contain confidential information	
Internal theft of information	Employee code of conduct and conflicts of interest addresses proprietary rights of the company and sanctions to be taken for breeches
Employee is not able to verify the identity of a client (e.g., phone masquerading)	

Sessão FRAAP

- Estabelecimento do nível de risco
  - Verificar se os elementos da equipa estão familiarizados com os termos e definições de Probabilidade e Impacto
  - Resumir as ameaças e controlos existentes
  - Caracterizar os níveis de avaliação para
    - Probabilidade
    - Impacto
  - Explicar os níveis de avaliação
    - Quando existe risco, os elementos tendem a classificar com nível máximo

Sessão FRAAP

- Estabelecimento do nível de risco
  - Definições e níveis de avaliação
    - Probabilidade

Term	*Definition*
Probability	Chance that an event will occur or that a specific loss value may be attained should the event occur
High	Very likely that the threat will occur within the next year
Medium	Possible that the threat may occur within the next year
Low	Highly unlikely that the threat will occur within the next year

    - Impacto

Term	*Definition*
Impact	A measure of the magnitude of loss or harm on the value of an asset
High	Entire mission or business impacted
Medium	Loss is limited to single business unit or objective
Low	Business as usual

Sessão FRAAP

- Estabelecimento do nível de risco
  - Definições e níveis de avaliação
    - Matriz de probabilidade x impacto
    - Caracterizar o risco residual

IMPACT

PROBABILITY

	High	Medium	Low
High	**A**	**B**	**C**
Medium	**B**	**B**	**C**
Low	**C**	**C**	**D**

A - Corrective action must be implemented
B - Corrective action should be implemented
C - Requires monitor
D - No action required at this time

Sessão FRAAP

- Estabelecimento do nível de risco
  - Avaliação das ameaças e controlos identificados

Threat	*Existing Control*	*Probability 1 = Low 2 = Medium 3 = High*	*Impact 1 = Low 2 = Medium 3 = High*	*Risk Level*
Confidentiality				
Insecure e-mail could contain confidential information		3	3	High
Internal theft of information	Employee code of conduct and conflicts of interest addresses proprietary rights of the company and sanctions to be taken for breeches	1	2	Low

Sessão FRAAP

- Identificar novos controlos ou melhoria dos existentes
  - Para os riscos que requerem essa necessidade
  - Identificados em conjunto com o owner
    - (vantagem em envolver os utilizadores)

Threat	*Existing Control*	*Probability 1 = Low 2 = Medium 3 = High*	*Impact 1 = Low 2 = Medium 3 = High*	*Risk Level*	*New or Enhanced Selected Control*
Confidentiality					
Insecure e-mail could contain confidential information		3	3	High	Information classification policy and handling standards are being implemented
Internal theft of information	Employee code of conduct and conflicts of interest addresses proprietary rights of the company and sanctions to be taken for breeches	1	2	Low	
Employee is not able to verify the identity of a client (e.g., phone masquerading)		1	1	Low	

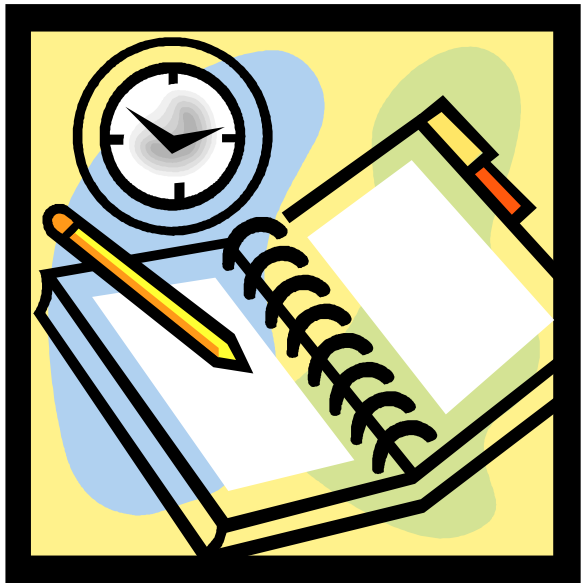
Sessão FRAAP

- Estabelecimento do nível de risco
  - Caracterizar novos níveis de risco

Threat	*Existing Control*	*Probability 1 = Low 2 = Medium 3 = High*	*Impact 1 = Low 2 = Medium 3 = High*	*Risk Level*	*New or Enhanced Selected Control*	*New Risk Level*
Confidentiality						
Insecure e-mail could contain confidential information		3	3	High	Information classification policy and handling standards are being implemented	Medium
Internal theft of information	Employee code of conduct and conflicts of interest addresses proprietary rights of the company and sanctions to be taken for breeches	1	2	Low		
Employee is not able to verify the identity of a client (e.g., phone masquerading)		1	1	Low		

Sessão FRAAP

- Estabelecimento do nível de risco
  - Prioritizar implementação de controlos
  - Planear essa implementação



Sessão FRAAP

- Estabelecimento do nível de risco
  - Na implementação de controlos, devem ser consideradas as normas e legislação em vigor:
    - Information Technology – Code of Pratice for Information Security Management (ISO/IEC 27002)
    - "Security Technologies for Manufacturing and Control Systems" (ISA-TR99.00.01-2004)
    - "Integrating Electronic Security into Manufacturing and Control Systems Environment" (ISA-TR99.00.02-2004)
    - Federal Information Processing Standards Publications (FIPS Pubs)
    - National Institute of Standards and Technology
    - CobiT® Security Baseline
    - Health Insurance Portability and Accountability Act (HIPAA)
    - The Basel Accords
    - Privacy Act of 1974
    - Gramm–Leach–Bliley Act (GLBA)
    - Sarbanes–Oxley Act (SOX)
    - "Information Security for Banking and Finance" (ISO/TR 13569)
    - FFEIC examination guidelines

Processo de análise de Risco FRAAP

- Post-FRAAP
  - Realizado pela equipa de consultores
    - Análise dos resultados da reunião
  - Pode ser necessário contactar alguns elementos da equipa
    - Através do gestor de projecto
    - Para algum esclarecimento adicional
    - Ou informação complementar

Processo de análise de Risco FRAAP

- Post-FRAAP
  - Relatório final
    - com sumário executivo
    - Resumo da reunião de equipa
    - Identificação de controlos complementares
    - Análise do processo
  - Apresentação das conclusões ao Gestor de Negócio

Deve ser muito parecido

Metodologias de Gestão de Risco

- Para suporte à Gestão de Risco podem ser utilizados referenciais como
  - ISO/IEC 27005 Information technology - Security techniques - Information security risk management
  - SP800-30 (NIST) - Risk Management Guide for Information Technology Systems
  - ISO 31000 - Risk management
  - Referenciais locais ou sectoriais como:
    - CRAMM (UK. Telcos)
    - Dutch A&K analysis (Holanda)
    - MAGERIT (Espanha)
    - MIGRA (Itália)

  - Link de referência: http://rm-inv.enisa.europa.eu/rm_ra_methods.html

AGENDA

- O processo de análise de risco FRAAP
  - Introdução
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP
  - Ferramentas de apoio ao processo

- **Identificação de ameaças e controlos para**
  - a Cibersegurança
  - a Privacidade
  - Serviços na Cloud

A Cibersegurança

- Cyber…
  - Cybercrime - criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime
  - Cybersafety - condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable
  - Cybersecurity = Cyberspace security - preservation of confidentiality, integrity and availability of information in the Cyberspace
  - Cyberspace - complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

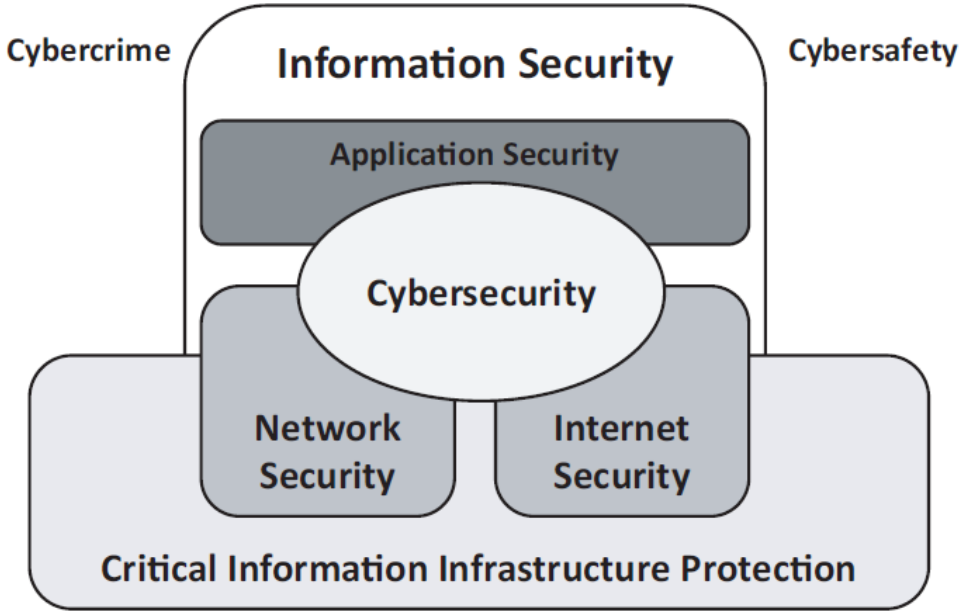
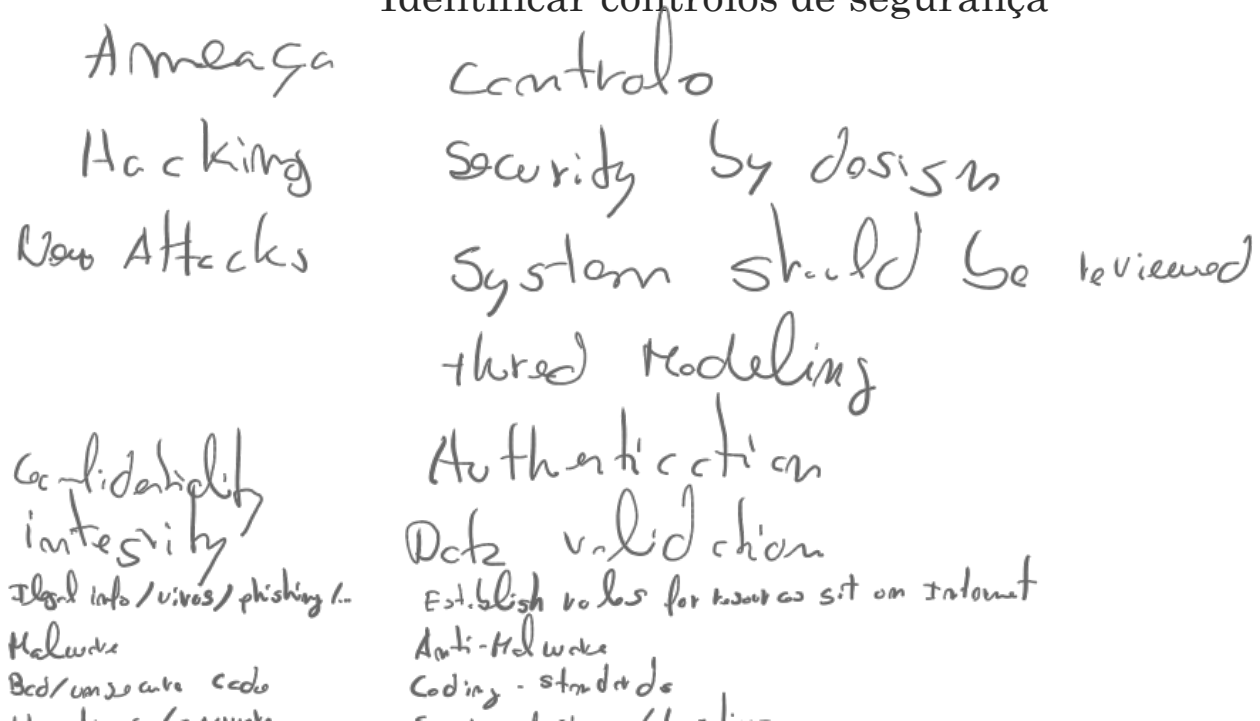


Figure 1 — Relationship between Cybersecurity and other security domains

A Cibersegurança

- Exercício
  - Identificar ameaças no Ciberespaço
    - 12.3 Server protection
    - 12.4 End-user controls
    - 12.5 Controls against social engineering attacks
  - Identificar controlos de segurança



Hackers / spyware
Spyware / malware
Vc confide / trata
Integrity / conf
Audability
Secure design / testing
Code signing
Adequate security controls
Store info securile
Visiliat vaquivamerts
Independently product under the common
Critori. schema

Privacidade

- Definidos requisitos em
  - Regulamneto Geral de Proteção de Dados
  - Lei n.º 58/2019 - Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados
  - ISO/IEC 27701 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
    - PII - personally identifiable information

Privacidade

- Exercício
  - Identificar ameaças de privacidade
    - 6.9.3.1 Backups
    - 6.12.1.2 Addressing security within supplier agreements
    - 6.13.1. Information Security incidente management
  - Identificar controlos de segurança

Segurança de serviços na cloud

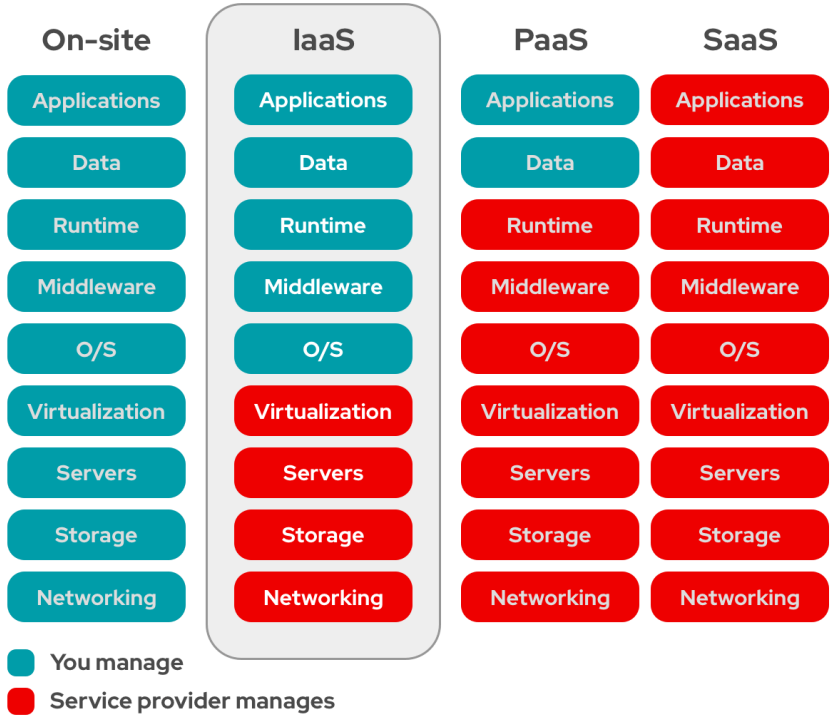
- Definidos requisitos em
  - ISO/IEC 27017 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Segurança de serviços na cloud

- Definições
  - 3.1.4 **cloud computing** - paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration
    - NOTE – Examples or resources include servers, operating systems, networking, software, and storage equipment.
  - 3.1.5 **cloud service** - one or more capabilities (3.1.2) offered via cloud computing (3.1.4) invoked using a declared interface
  - 3.1.6 **cloud service category** - group of cloud services (3.1.5) that possess some qualities in common with each other
  - 3.1.7 **cloud service customer** - party (3.1.13) which is in a business relationship for the purpose of using cloud services (3.1.5)
  - 3.1.8 **cloud service provider** - party (3.1.13) which makes cloud services (3.1.5) available
  - 3.1.9 **cloud service user** - person associated with a cloud service customer (3.1.7) that uses cloud services (3.1.5)

Segurança de serviços na cloud

- Definições
  - 3.1.10 **IaaS (Infrastructure as a Service)** - cloud service category (3.1.6) in which the cloud capabilities type (3.1.3) provided to the cloud service customer (3.1.7) is an infrastructure capabilities type (3.1.11)
  - 3.1.12 **PaaS (Platform as a Service)** - cloud service category (3.1.6) in which the cloud capabilities type (3.1.3) provided to the cloud service customer (3.1.7) is a platform capabilities type (3.1.14)
  - 3.1.15 **SaaS (Software as a Service)** - cloud service category (3.1.6) in which the cloud capabilities type (3.1.3) provided to the cloud service customer (3.1.7) is an application capabilities type (3.1.1)



Segurança de serviços na cloud

- Interpretação da norma
  - Para determinados controlos do Anexo A da ISO 27001

A.6.1.3	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.

  - Apresenta requisitos acrescidos, na ótica do
    - cloud service customer
    - cloud service provider

6.1.3 Contact with authorities

Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should identify the authorities relevant to the combined operation of the cloud service customer and the cloud service provider.	The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data.

Privacidade

- Exercício
  - Identificar ameaças de privacidade
    - 12.3.1 Information backup
    - 15.1.2 Addressing security within supplier agreements
    - 16.1. Information security incident management
  - Identificar controlos de segurança

Segurança e Gestão de Risco

2ºSem 2023/24

O Processo FRAAP

LUIS AMORIM

23 Mar 2024