SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

MODELO DE SEGURANÇA INTEGRADO

PROCESSO DE AVALIAÇÃO DOS RISCOS

LUIS AMORIM

09 Abr 2022

2 AGENDA

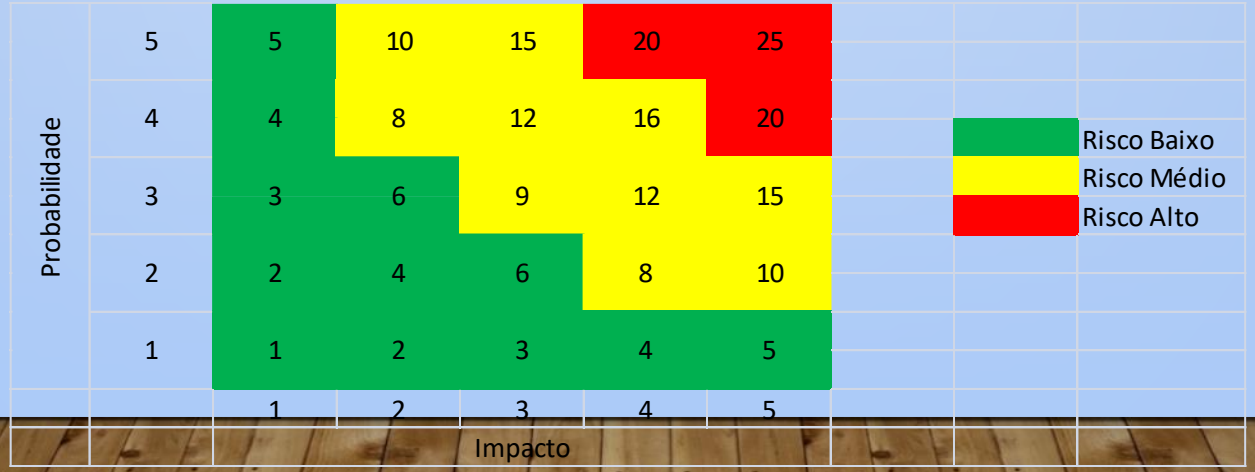
- **O processo de análise de risco FRAAP (9 Abr)**
  - Introdução
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP

3 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

4 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 dos ativos no cálculo resulta num valor final difícil de interpretar
    - Podem ser definidos níveis para medição, mas a interpretação ser qualitativa



5 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.

6 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

7 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

8 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
    - consultor com conhecimento do FRAAP
  - Escriba ou secretário(a)
    - responsável por documentar as reuniões
  - Especialistas relacionados com o objecto
    - Negócio
    - IT
    - Users

9 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

10 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

11 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

12 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

13 PROCESSO DE ANÁLISE DE RISCO FRAAP

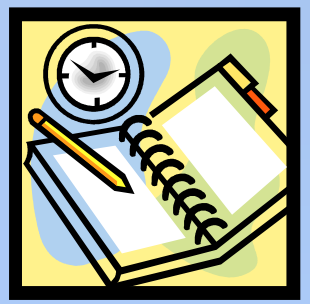
- Antes de iniciar deve existir um Programa de Sensibilização
  - Dar a conhecer o processo
  - Envolver os participantes
  - Este Programa deve ser conduzido de forma a
    - Avaliar o conhecimento relativo a avaliação de risco
    - Determinar o que os gestores e outros funcionários pretendem aprender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

14 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

15 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



16 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

17 SESSÃO PRE-FRAAP

- Resultados esperados
  1. (pré) Triagem
  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
  7. Mini-Brainstorming

18 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

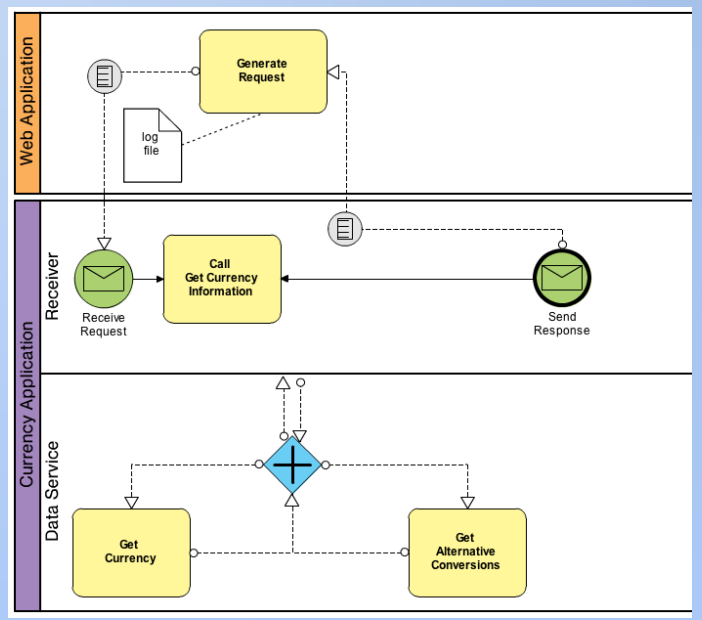
Impacto / Sensibilidade	Alto	Médio	Baixo
Alto	Avaliação Risco	Avaliação Risco	Avaliação Risco
Médio	Avaliação Risco	Avaliação Risco	Implementar Controlos base
Baixo	Avaliação Risco	Implementar Controlos base	n.a.

19 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

20 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



21 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

22 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

23 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)*	

25 AGENDA

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

26 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

27 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

28 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

29 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

30 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

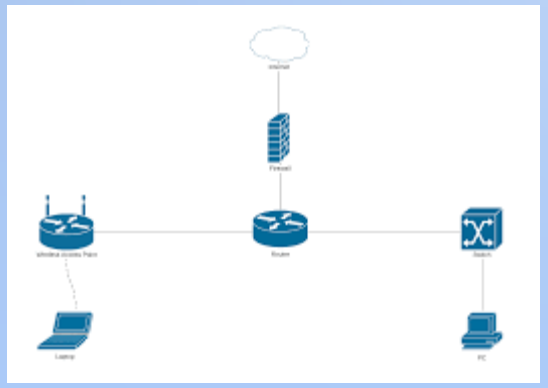
FRAP Session Agenda	Responsibility
• Introduction	
• **Explain the FRAP process and cover definitions**	• Owner + Facilitator
• **Review scope statement**	• Owner
• Review Visual Diagram	• Technical support
• Discuss definitions	• Facilitator

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

• Identify roles and introduction	• Team
• Review session agreements	

31 SESSÃO FRAAP

- Sessão de trabalho - Introdução
  - Review Visual Diagram – Technical support
    - Deve fazer a apresentação do diagrama, explicando o processo
    - Cerca de 5 min.



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	

32 SESSÃO FRAAP

- Sessão de trabalho - Introdução
  - 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

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	

33 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

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	

34 SESSÃO FRAAP

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

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	

35 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)

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**	

36 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

FRAP Session Agenda	Responsibility
• Introduction	
• **Brainstorm for threats**	• Team
• Establish risk levels (probability and impact)	• Team
• Prioritize threats	• Team
• Identify possible safeguards	• Team
• Create Management Summary Report	• Facilitator

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

37 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

38 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

39 SESSÃO FRAAP

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

40 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	

41 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

42 SESSÃO FRAAP

- Antes do próximo ponto, fazer pausa
  - Dá oportunidade para
    - Verificar mensagens
    - Tomar um café
    - Limpar
  - A equipa fica a organizar informação

  e a preparar fase seguinte

43 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)	

44 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

45 SESSÃO FRAAP

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

Nível	Probabilidade	Descrição	Column1
1	Baixo	Não é provável que aconteça	< 1
2	Médio	Pode acontecer raras vezes	1 a 2
3	Alto	Pode acontecer algumas vezes	3 a 4
4	Muito Alto	Práticamente certo que irá acontecer, e vai repetir-se	> 4

    - Impacto

Nível	Impacto	Descriçao do Impacto
1	Baixo	Um posto de trabalho afectado
2	Médio	Mais que um posto de trabalho afectado
3	Alto	Afetou o ambiente de desenvolvimento, mas pode ser reposto
4	Muito Alto	Comprometeu todo o processo de desenvolvimento

46 SESSÃO FRAAP

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

Impacto / Probabilidade	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

47 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

48 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	

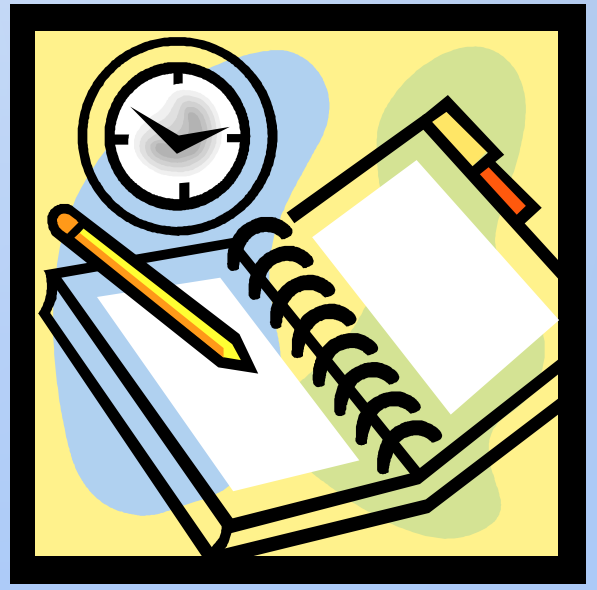
49 SESSÃO FRAAP

- 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		

50 SESSÃO FRAAP

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



51 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

52 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

53 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

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

MODELO DE SEGURANÇA INTEGRADO

PROCESSO DE AVALIAÇÃO DOS RISCOS

LUIS AMORIM

28 Mai 2022