

Segurança e Gestão de Risco

2ºSem 2023/24

FRAAP

LUIS AMORIM

18 Mai 2024

AGENDA

- Trabalhos de grupo
 - Relatório - Estrutura
- FRAAP
 - Exercício prático
 - FRAAP

Trabalhos de Grupo

- Grupos constituídos
 - Grupo A
 - Ana Raquel Paradinha - 102491
 - João Miguel Matos – 103341
 - ?
 - Grupo B
 - Bruna Simões - 103453
 - Daniel Ferreira - 102442
 - Tiago Carvalho – 104142
 - Grupo C
 - José João Alexandre - 118373
 - Rafael Oliveira – 117240
 - Gonçalo Marques
- Grupos candidatados
 - Grupo D
 - Ana Vidal
 - Simão Andrade
 - Wilmara Francisco
 - Grupo E
 - Filipe Silveira
 - Ricardo Covelo
 - Telmo Sauce
 - Grupo F
 - Diogo Almeida
 - Fábio Ferreira
 - Rafael Oliveira
 - Grupo G
 - Filipe Antão - 103470
 - Paulo Pinto - 103234
 - Diogo Silveira – 85117
 - Grupo H
 - Diogo Maia - 111707
 - Francisco Cunha - 114661
 - Luis Peixoto - 115447

Análise e Avaliação de Riscos

- Exercício Prático FRAAP (27Abr)
 - AETTUA
 - *Miguel Matos*
 - *José Andrade*
 - Diogo Silveira
 - Web site Ecomm (grupo D ?)
 - Ana Vidal
 - Simão Andrade
 - Wilmara Francisco
 - Site Apostas (Grupo E ?)
 - Filipe Silveira
 - Ricardo Covelo
 - Telmo Sauce

Trabalhos de Grupo

- Plano – Avaliação dos Riscos
 - pré-FRAAP
 - A realizar entre 27 e 31 de Maio
 - Acertar data da sessão de FRAAP
 - Enviar relatório até dia 01 de Junho
 - Reuniões FRAAP
 - Entre 03 e 11 de Jun
 - Relatório de FRAAP
 - Descrição e conclusões da avaliação
 - Com Sumário Executivo
 - Enviar até dia 15 de Junho
 - Apresentação das conclusões
 - Colocar em slide as principais conclusões
 - extrair do Sumário Executivo
 - Data de apresentação: dia **17 de Junho**– a confirmar
- Plano - Vulnerability scanner
 - Preparação
 - Assistir à sessão relativa ao mesmo sistema
 - Correr ferramentas
 - Combinar com cliente (feriado ou fds)
 - Até 10 de Junho
 - Descrição e conclusões da avaliação
 - Com Sumário Executivo
 - Relatório até 15 de Junho
 - Alinhado com relatório FRAAP
 - Apresentação das conclusões
 - Colocar em slide as principais conclusões
 - extrair do Sumário Executivo
 - Data de apresentação: dia **17 de Junho**– a confirmar

Sumário Executivo

- Exemplo de Sumário executivo
 - 1 (a 2) páginas
 - Principais conclusões
 - Apelando (e apontando) para o resto do documento

Sumário Executivo

Listas de participantes no processo

Equipa Responsável pela reunião FRAAP:



Equipa da trust:



Resumo do âmbito e princípios estabelecidos

O processo, seguindo a metodologia FRAPP começou com uma reunião Pré-FRAAP, realizada no dia 11/06/2022, onde foram abordados e explicados os modelos em que ia decorrer a avaliação de risco do sistema De-Risk. Aqui foram identificados alguns riscos assim como foi passada informação base sobre o projeto, tanto pela explicação verbal como com o auxílio de um diagrama, os objetivos também foram transmitidos. Foi também acordada a metodologia de classificação dos riscos. No final da reunião ficou assente a participação do responsável do projeto, assim como um responsável técnico e utilizadores da solução.

A reunião FRAAP aconteceu no dia 29/06/2022 com a participação do responsável do projeto e com um responsável técnico, não estiveram presentes utilizadores durante a reunião. A reunião demorou cerca de 2 horas e 20 minutos e contou com a presença de outro grupo com um projeto ligado a mesma solução. Durante a reunião foram identificadas ameaças e no final foram feitas 2 análises completas para 2 riscos identificados (probabilidade, impacto, controlos existentes, novos controlos e novo cálculo do risco depois dos controlos). A tabela final ficou por preencher com o responsável do projeto e com o responsável técnico a assumirem a responsabilidade de a entregarem dia 4 ou 5 de julho.

A produção deste relatório e análise de resultados é resultado da terceira fase do processo FRAAP.

Resumo da metodologia

A metodologia seguida já mencionada assenta numa avaliação de risco eficiente, que se destaca pela avaliação de um sistema/processo em termos de dias em vez de semanas ou meses. Esta metodologia tem 3 grandes fases, passamos a explicar cada uma.

A fase de Pré-FRAAP tem como procedimento uma reunião de 1 hora e 30 minutos como tempo máximo no qual vão ser definidas as bases de trabalho para as fases seguintes. A reunião FRAAP (próxima fase) não deve demorar mais de 4 horas e devem ser identificadas ameaças para a

Sumário Executivo

- Exemplo de Sumário executivo
 - 1 (a 2) páginas
 - Principais conclusões
 - Apelando (e apontando) para o resto do documento

solução, os controlos que existem, uma avaliação do nível do risco e para além disso devem ser pensados novos controlos para mitigar riscos. No final deverá ser produzido um relatório com as conclusões da análise.

Resumo das principais conclusões da avaliação

Os riscos mais significativos que foram identificados passam por:

- Bugs de programação levarem a inconsistência dos dados
 - Controlo: Processo de desenvolvimento bem definido
- Utilização por terceiros de sessão exposta, sem vigilância por parte do utilizador
 - Controlo de implementação de timeout

Ambos com controlos implementados mas que ainda resultam em riscos que devem ser analisados.

Referenciação à restante documentação

[Referência ao PDF do Pré-FRAAP](#)

[Referência ao Excel com a metodologia e com a tabela de riscos \(Que eles enviaram\)](#)

[Referência ao Excel com a metodologia e com a tabela de riscos \(Que completamos com os novos controlos\)](#)

[Referência a apresentação Pré-FRAAP](#)

Conclusões

O processo de um ponto de vista da metodologia decorreu com algumas restrições, devido a falhas na comunicação entre os responsáveis pelo processo FRAAP e os responsáveis do projeto da Trust, e a limitação da reunião FRAAP, o ponto central da avaliação, onde apenas compareceram 2 pessoas quando o processo deveria incluir 10 a 20, sendo que também não pudemos contar com utilizadores da plataforma, o que resultaria numa avaliação mais criteriosa. Todos estes pontos devem ser tidos em conta quando consideramos os riscos recolhidos.

Por constrangimentos da Trust, a informação recebida tardeamente não vinha completamente preenchida, nomeadamente:

- Identificação superficial dos controlos implementados (ex: "Existe controlo" e "Não é Risco")
- Não foram identificados os novos controlos a implementar para os riscos mais elevados.

Tentámos complementar a análise com alguns controlos adicionais mas estes estão sempre limitados ao conhecimento que temos da solução e fogem à prática do processo FRAAP, baseada no envolvimento dos colaboradores da empresa durante o processo.

Controlos a considerar e um plano de acção/priorização

De forma a mitigar os riscos identificados e sugerido:

- Sensibilização dos colaboradores a seguir boas práticas de secretismo da informação
- Criação de um novo papel para manter o princípio do menor privilégio
- Uso de canais secundários para restringir acesso a certos documentos
- Entre outros definidos mais à frente

Trabalhos de Grupo

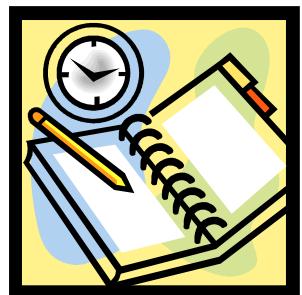
- Avaliação
 - Fase Inicial (20%)
 - Condução da reunião + documento com conclusões da sessão inicial (Pre-Fraap ou ferramentas)
 - Realização da Atividade (30%)
 - Reunião FRAAP
 - Ferramentas utilizadas
 - Relatório Final (40%)
 - Apresentação dos resultados (10%)
 - 3 a 4 slides com resumo do relatório

AGENDA

- Trabalhos de grupo
 - Relatório - Estrutura
- FRAAP
 - Exercício prático
 - FRAAP

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

- Pre-FRAAP

- Resultados esperados
 - (pré) Triagem dos sistemas/processos
 - Definição do âmbito
 - Diagrama com a descrição/detalhe do sistema ou processo a avaliar
 - Identificação dos intervenientes/equipa a incluir no processo
 - Requisitos para a reunião FRAAP (planeamento, sala, materiais)
 - Acordar definições de princípio
 - Mini-Brainstorming (identificar ameaças para introdução na reunião FRAAP)

ISSUE
PRIOR TO THE MEETING
1. Date of Pre-FRAAP Meeting <i>Record when and where the meeting is scheduled</i>
2. Project Executive Sponsor or Owner <i>Identify the owner or sponsor who has executive responsibility for the project</i>
3. Project Leader <i>Identify the individual who is the primary point of contact for the project or asset under review</i>
4. Pre-FRAAP Meeting Objective <i>Identify what you hope to gain from the meeting – typically the seven deliverables will be discussed</i>
5. Project Overview <i>Prepare a project overview for presentation to the pre-FRAAP members during the meeting</i> Your understanding of the project scope The FRAAP methodology Milestones Pre-screening methodology
6. Assumptions <i>Identify assumptions used in developing the approach to performing the FRAAP project</i>
7. Pre-screening Results <i>Record the results of the pre-screening process</i>
DURING THE MEETING
8. Business Strategy, Goals and Objectives <i>Identify what the owner's objectives are and how they relate to larger company objectives</i>
9. Project Scope <i>Define specifically the scope of the project and document it during the meeting so that all participating will know and agree</i>
<ul style="list-style-type: none"> • Applications/Systems • Business Processes • Business Functions • People and Organizations • Locations/Facilities
10. Time Dependencies <i>Identify time limitations and considerations the client may have</i>
11. Risks/Constraints <i>Identify risks and/or constraints that could affect the successful conclusion of the project</i>
12. Budget <i>Identify any open budget/funding issues</i>
13. FRAAP Participants <i>Identify by name and position the individuals whose participation in the FRAAP session is required</i>
14. Administrative Requirements <i>Identify facility and/or equipment needs to perform the FRAAP session</i>
15. Documentation <i>Identify what documentation is required to prepare for the FRAAP session (provide the client the FRAAP Document Checklist)</i>

ISSUE	DURING THE MEETING
PRIOR TO THE MEETING	
1. Date of Pre-FRAAP Meeting <i>Record when and where the meeting is scheduled</i>	8. Business Strategy, Goals and Objectives <i>Identify what the owner's objectives are and how they relate to larger company objectives</i>
2. Project Executive Sponsor or Owner <i>Identify the owner or sponsor who has executive responsibility for the project</i>	9. Project Scope <i>Define specifically the scope of the project and document it during the meeting so that all participating will know and agree</i>
3. Project Leader <i>Identify the individual who is the primary point of contact for the project or asset under review</i>	<ul style="list-style-type: none"> • Applications/Systems • Business Processes • Business Functions • People and Organizations • Locations/Facilities
4. Pre-FRAAP Meeting Objective <i>Identify what you hope to gain from the meeting – typically the seven deliverables will be discussed</i>	10. Time Dependencies <i>Identify time limitations and considerations the client may have</i>
5. Project Overview <i>Prepare a project overview for presentation to the pre-FRAAP members during the meeting</i>	11. Risks/Constraints <i>Identify risks and/or constraints that could affect the successful conclusion of the project</i>
Your understanding of the project scope	12. Budget <i>Identify any open budget/funding issues</i>
The FRAAP methodology	13. FRAAP Participants
Milestones	<i>Identify by name and position the individuals whose participation in the FRAAP session is required</i>
Pre-screening methodology	14. Administrative Requirements
6. Assumptions <i>Identify assumptions used in developing the approach to performing the FRAAP project</i>	<i>Identify facility and/or equipment needs to perform the FRAAP session</i>
7. Pre-screening Results <i>Record the results of the pre-screening process</i>	15. Documentation <i>Identify what documentation is required to prepare for the FRAAP session (provide the client the FRAAP Document Checklist)</i>

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

14

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



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 <ul style="list-style-type: none"> • 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

17

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 Statement 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 papéis
 - 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 registrar a ideia, antes de discuti-la
 - Assegurar que o escribe assenta todas as questões
 - Uma temática (C-I-D) de cada vez
 - Limite de tempo por ativo/atividade (3 a 5 minutos)



22

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 secretaria

Conversas fora do escritório podem divulgar informação sensível

23

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

29

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

<i>Threat</i>	<i>Existing Control</i>
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 breaches
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
 - Impacto

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

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		
		High	Medium	Low
PROBABILITY	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

<i>Threat</i>	<i>Existing Control</i>	<i>Probability</i> 1 = Low 2 = Medium 3 = High	<i>Impact</i> 1 = Low 2 = Medium 3 = High	<i>Risk Level</i>
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)

<i>Threat</i>	<i>Existing Control</i>	<i>Probability</i> 1 = Low 2 = Medium 3 = High	<i>Impact</i> 1 = Low 2 = Medium 3 = High	<i>Risk Level</i>	<i>New or Enhanced Selected Control</i>
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	

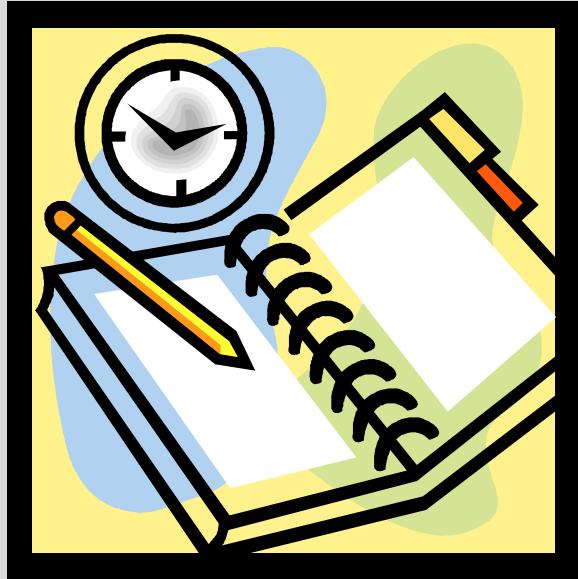
Sessão FRAAP

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

<i>Threat</i>	<i>Existing Control</i>	<i>Probability</i> 1 = Low 2 = Medium 3 = High	<i>Impact</i> 1 = Low 2 = Medium 3 = High	<i>Risk Level</i>	<i>New or Enhanced Selected Control</i>	<i>New Risk Level</i>
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
 - Prioritzar 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 Practice 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

Sessão FRAAP

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

<i>Threat</i>	<i>Existing Control</i>	<i>Probability</i> 1 = Low 2 = Medium 3 = High	<i>Impact</i> 1 = Low 2 = Medium 3 = High	<i>Risk Level</i>
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

- Tratamento dos riscos
 - 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)

<i>Threat</i>	<i>Existing Control</i>	<i>Probability</i> 1 = Low 2 = Medium 3 = High	<i>Impact</i> 1 = Low 2 = Medium 3 = High	<i>Risk Level</i>	<i>New or Enhanced Selected Control</i>
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 breaches	1	2	Low	
Employee is not able to verify the identity of a client (e.g., phone masquerading)		1	1	Low	

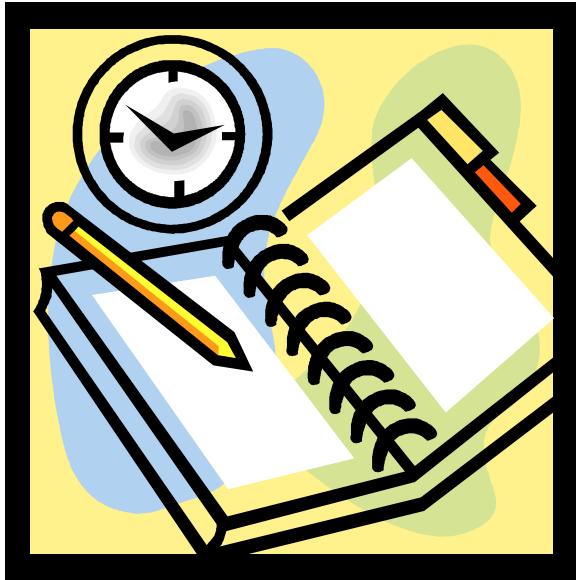
Sessão FRAAP

- Tratamento dos riscos
 - Calcular os novos níveis de risco
 - Considerando a implementação dos controlos identificados

<i>Threat</i>	<i>Existing Control</i>	<i>Probability</i> 1 = Low 2 = Medium 3 = High	<i>Impact</i> 1 = Low 2 = Medium 3 = High	<i>Risk Level</i>	<i>New or Enhanced Selected Control</i>	<i>New Risk Level</i>
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

- Tratamento dos Riscos
 - Prioritzar implementação de controlos
 - Planear essa implementação



Sessão FRAAP

- Tratamento dos Riscos
 - Na implementação de controlos, devem ser consideradas as normas e legislação em vigor:
 - Information Technology – Code of Practice 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 (alunos)
 - 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
- Resultados esperados
 - Relatório final
 - com sumário executivo
 - Resumo da reunião de equipa
 - Identificação de controlos complementares
 - Análise do processo
 - Apresentação das conclusões ao Gestor de Negócio



Processo de análise de Risco FRAAP

- Sumário executivo (composição)
 - Lista de participantes no processo
 - Resumo do âmbito e princípios estabelecidos
 - 2 ou 3 parágrafos com um resumo de como decorreu o processo
 - Onde e quando decorreu
 - Identificar constrangimentos e factos assumidos
 - Resumo da metodologia
 - Resumo das principais conclusões da avaliação
 - Maiores riscos e controlos
 - Referenciação à restante documentação
 - Conclusões
 - Visão sobre o processo todo
 - Controlos a considerar e um plano de acção /prioritização

Análise e Avaliação de Riscos

- Exercício Prático FRAAP
 - AETTUA
 - Miguel
 - José Andrade
 - Diogo Silveira
 - Web site Ecom
 - Ana Vidal
 - Simão Andrade
 - Wilmara Francisco
 - Site Apostas
 - Filipe
 - Ricardo Covelo
 - Telmo Sauce

Exercício prático

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

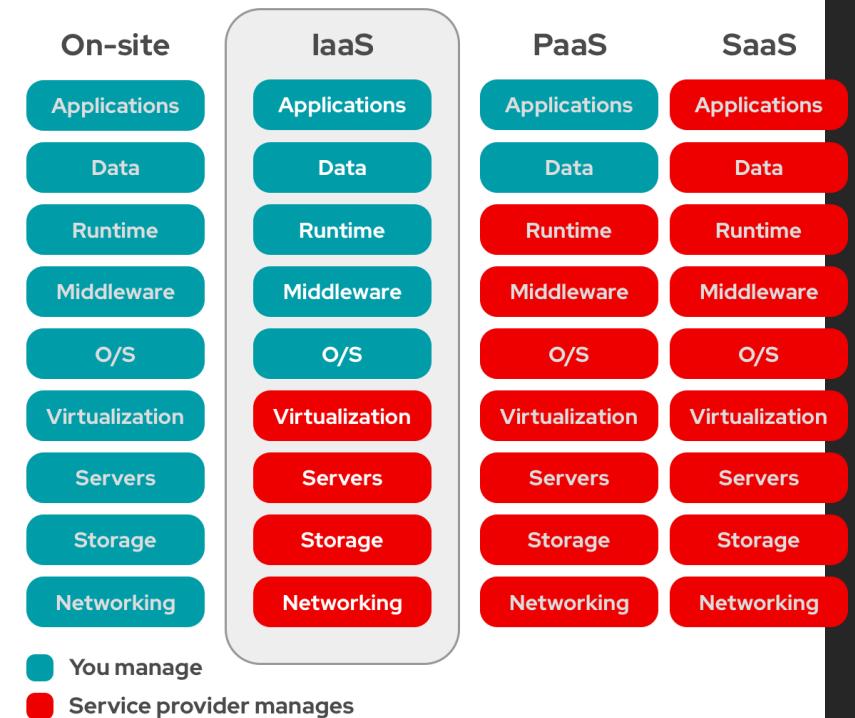
Segurança de serviços na cloud

- 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)

50

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	<i>Control</i> Appropriate contacts with relevant authorities shall be maintained.
• Apreser <ul style="list-style-type: none"> • 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.

Segurança e Gestão de Risco

2ºSem 2023/24

FRAAP

LUIS AMORIM

27 Abr 2024

52

