SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

FRAAP E AMEAÇAS E CONTROLOS ESPECÍFICOS DE SEGURANÇA

LUIS AMORIM

14 Mai 2022

2 AGENDA

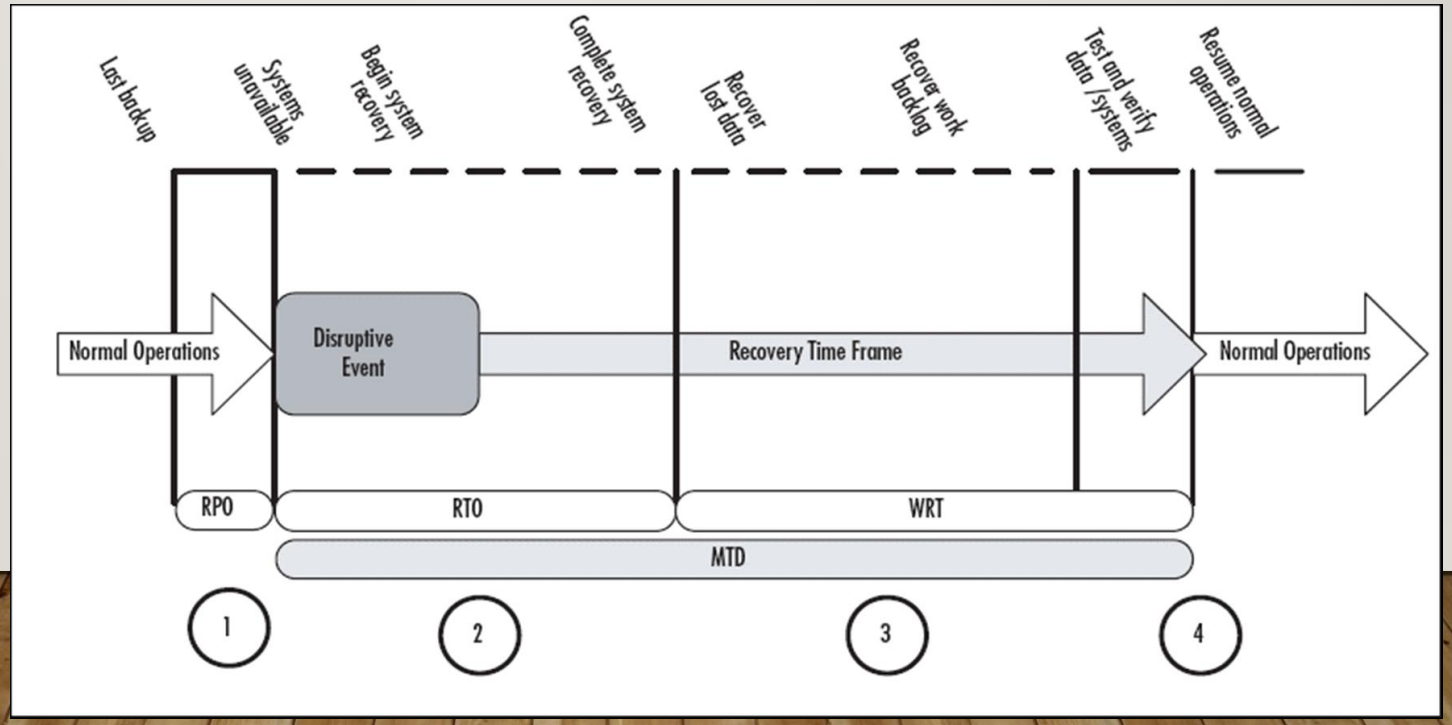
- Revisão da aula anterior
  - Business Impact Analysis(BIA)
  - GAP Analisys
  - Definir uma Política de Segurança
- Processo de análise de risco FRAAP
- Identificação de ameaças e controlos para
  - a Cibersegurança
  - a Privacidade
  - Serviços na Cloud

3 BUSINESS IMPACT ANALYSIS (BIA)

- Um processo de Business Impact Analysis pretende determinar os impactos que um incidente disruptivo tem na operação e na viabilidade dos processos core de negócio
- Implica antes
  - Determinar os processos core
  - Determinar quais são os principais recursos utilizados por esses processos
    - Aplicações; Sistemas; Processos; Funções; Pessoas
- Depois
  - Classificar esses recursos (em termos de importância e prioridade)
  - Caraterizar os requisitos de recuperação

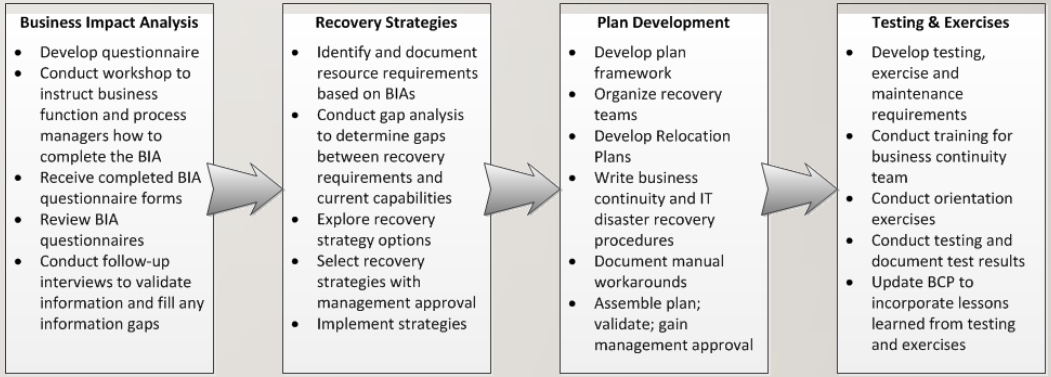
4 BUSINESS IMPACT ANALYSIS (BIA)

- Caraterizar os requisitos de recuperação
  - R P O = Recovery Point Objective - maximum acceptable amount of data loss measured in time
  - R T O = Recovery Time Objective - the maximum tolerable amount of time needed to bring all critical systems back online
  - W R T = Work Recovery Time - the maximum tolerable amount of time that is needed to verify the system and/or data integrity
  - M T D = Maximum Tolerable Downtime - total amount of time that a business process can be disrupted without causing any unacceptable consequences



5 BUSINESS IMPACT ANALYSIS(BIA)

- Aplicar os resultados do BIA
  - Para estabelecer estratégias de recuperação
  - Estabelecer ou rever os planos de Continuidade
    - Se o tempo máximo de *downtime* for inferior ao definido anteriormente



6 GAP ANALYSIS

- GAP Analysis consiste na comparação entre o estado presente e o estado desejado (futuro)

- Para tal é preciso resposta para:
  - Qual o estado pretendido
    - Ou estado "compliant",
    - quando numa auditoria/certificação
  - Qual o estado actual

  - O que é preciso ser feito

1 SCOPE			Comments
This international standard establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.			
2 TERMS DEFINITIONS			
For better understanding, ISO 27002 identifies and defines key information security terms.			
3 STRUCTURE OF THIS STANDARD			
This standard contains eleven (11) chapters containing 38 control areas.			
4 RISK ASSESSMENT AND TREATMENT			
The information security risk assessment should have a clearly defined scope.			
5 SECURITY POLICY Note: ISO17799 Sections 1, 2 and 3 are non-action items, and are not included as checklist items.			
5.1 Information Security Policy	Management direction and support for information security must be clearly established.		
5.1.1 Information Security Policy Document	Has an information security policy been approved by management?	Y ___ N ___	
	Has an information security policy been implemented?	Y ___ N ___	
	Has an information security policy been communicated to all employees?	Y ___ N ___	
5.1.2 Review of the Information Security Policy	Has the Information Security Policy been assigned an Owner?	Y ___ N ___	
	Has a policy review process been established?	Y ___ N ___	

7 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- Desenvolvimento da Política de Segurança
  - Organização
  - A Política de Segurança deverá ser desdobrada em documentos auxiliares que apresentam princípios e orientações mais específicas e dirigidas a grupos de funcionários ou a funções determinadas (por exemplo, orientações sobre reportar incidentes de segurança deverão ser dirigidas a todos os funcionários, políticas especificas relativamente à administração de sistemas destinam-se apenas aos técnicos da Informática).
  - Exemplos de Políticas
    - Política de Classificação de Informação
    - Política de Uso aceitável
    - Política de Controlo de Acessos
    - Política de Backups
    - Política de Teletrabalho e de Acesso Remoto
    - Política de controlos criptográficos
    - Política de Fornecedores

8 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- Exemplo de **Política** de Backups

1. Política de Backup

1. Realização dos backups

Para salvaguardar a informação contida no servidor e respetivos projetos, existe uma politica de backups definida, que passa por realizar backup a todas as máquinas virtuais onde estão inseridos todos os dados relativos aos projetos. Desta forma, garante-se que aquando da necessidade de aceder a um dos backups todos os dados estão com o formato desejado.

Assim, são realizados backups incrementais

Para salvaguardar a informação relativa aos projetos de desenvolvimento seguro e do Sistema de Gestão de Segurança da Informação, deverão ser realizados os seguintes backups:

- Backup ao servidor principal onde é executado o ambiente de virtualização;
- Backup de cada uma das máquinas virtuais (projetos) existentes no ambiente de virtualização;

Cada um dos backups anteriores deve ser realizado de acordo com o seguinte ciclo:

- Full Backups todas as 2as feiras;
- Backups incrementais entre 3ª e 6ª feira

Estes backups devem ser realizados no final do dia de trabalho, ao final do dia.

Caso se verifique um erro na realização de uma tarefa de backup, este deve ser ranalisado pelo Gestor de Projeto e decidida qual a melhor forma de o realizar, nomeadamente na próxima pausa, por exemplo hora de almoço.

9 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- **Procedimento** de Backups

1. Procedimento de Backups

A realização dos backups será executada através da ferramenta "*BackUp Maker*", que deve estar configurada de forma a satisfazer a política de realização de backups.

É responsabilidade da Equipa de Operação IT garantir a sua realização, através da configuração e monitorização da ferramenta.

1.1. Validação dos Backups

De modo a validar-se a execução dos backups deve-se aceder ao servidor e validar-se através do relatório da aplicação "*BackUp Maker*" se os backups foram realizados com sucesso.
Caso os mesmos tenham sido realizados com sucesso deve-se continuar a execução das tarefas conforme o previsto. Em caso de erro deve-se tentar executar os mesmos de forma manual e verificar se o problema volta a ocorrer. Se o erro voltar a acontecer, deve-se proceder à reconfiguração dos backups de modo a garantir o normal funcionamento dos mesmos.
O diagrama seguinte ilustra o que foi descrito nos parágrafos anteriores.

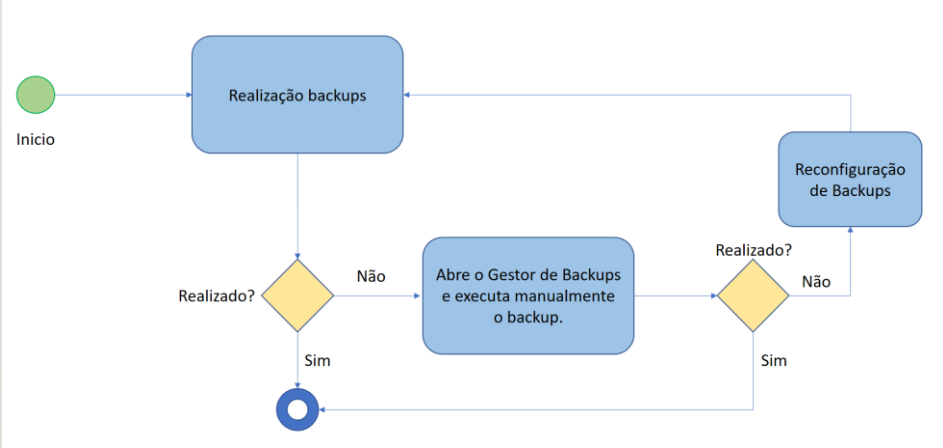


Figura 1 - Workflow de validação dos Backups

10 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- **Exercício prático**
  - Desenvolver práticas de Salvaguarda de informação
    - Definir **Política de Controlo de Acessos**
    - Definir **Procedimentos de Operação**, alinhados com essa política

11 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- (da ISO 27002)
  - **9.1.1 Access control policy**
  - Implementation guidance
    - Asset owners should determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks.
    - Access controls are both logical and physical (see Clause 11) and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

12 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- **9.1.1 Access control policy** (da ISO 27002)
  - The policy should take account of the following:
    - **a) security requirements of business applications;**
    - b) policies for information dissemination and authorization, e.g. the need-to-know principle and information security levels and classification of information (see 8.2);
    - c) consistency between the access rights and information classification policies of different systems and networks;
    - d) relevant legislation and any contractual obligations regarding limitation of access to data or services (see 18.1);
    - e) management of access rights in a distributed and networked environment which recognizes all types of connections available;
    - **f) segregation of access control roles, e.g. access request, access authorization, access administration;**
    - **g) requirements for formal authorization of access requests (see 9.2.1 and 9.2.2);**
    - **h) requirements for periodic review of access rights (see 9.2.5);**
    - **i) removal of access rights (see 9.2.6);**
    - j) archiving of records of all significant events concerning the use and management of user identities and secret authentication information;
    - **k) roles with privileged access (see 9.2.3).**

13 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

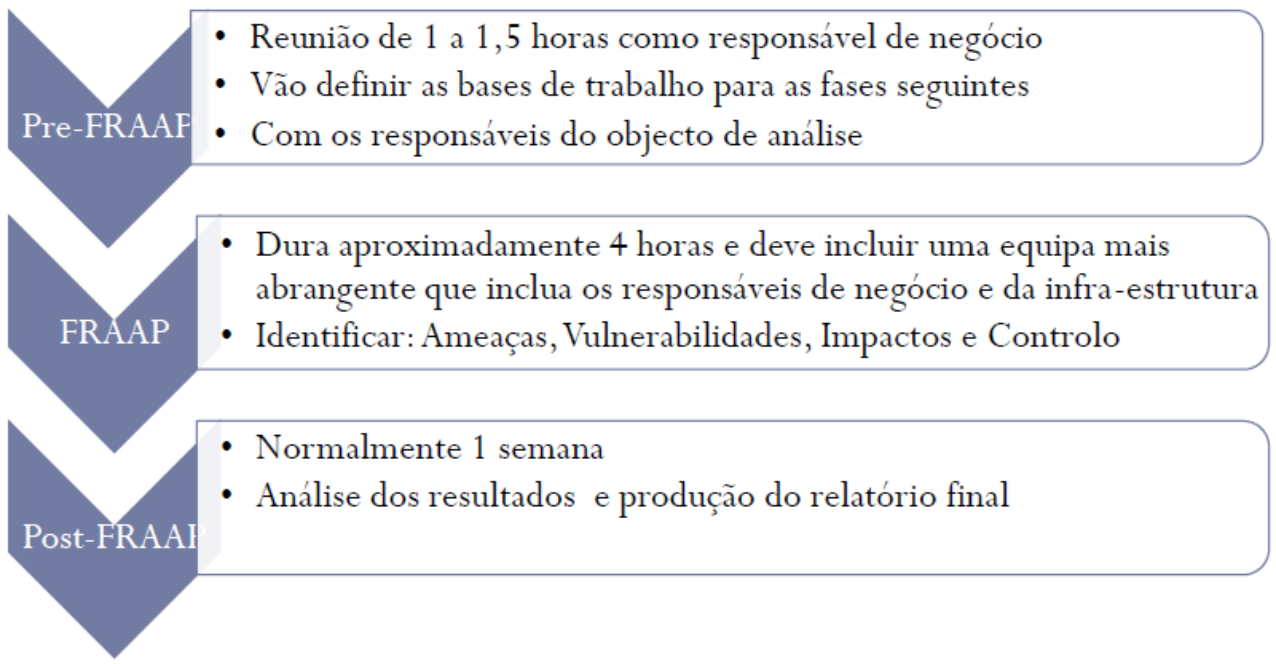
- **9.1.1 Access control policy** (da ISO 27002)
  - Other information
  - Care should be taken when specifying access control rules to consider:
    - **a) establishing rules based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";**
    - b) changes in information labels (see 8.2.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;
    - **c) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;**
    - d) rules which require specific approval before enactment and those which do not.
    - Access control rules should be supported by formal procedures (see 9.2, 9.3, 9.4) and defined responsibilities (see 6.1.1, 9.32, 15.1).
    - Role based access control is an approach used successfully by many organisations organizations to link access rights with business roles.

14 AGENDA

- Revisão da aula anterior
  - Business Impact Analysis(BIA)
  - GAP Analisys
  - Definir uma Política de Segurança
- ➢ Processo de análise de risco FRAAP
- Identificação de ameaças e controlos para
  - a Cibersegurança
  - a Privacidade
  - Serviços na Cloud

15 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Facilitated Risk Analysis and Assessment Process



16 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Pre-FRAAP
  - Resultados esperados
    - ~~Pré-triagem dos resultados esperados~~
    - 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 principio
    - Mini-Brainstorming (identificar ameaças para introdução na reunião FRAAP)

ISSUE
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*

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)*

17 SESSÃO FRAAP

- FRAAP
  - Resultados esperados
    - Identificação das Ameaças
    - Identificação das Vulnerabilidades
    - Identificação dos Controlos Existentes
    - Caracterização dos Riscos Residuais

18 SESSÃO FRAAP

- Agenda

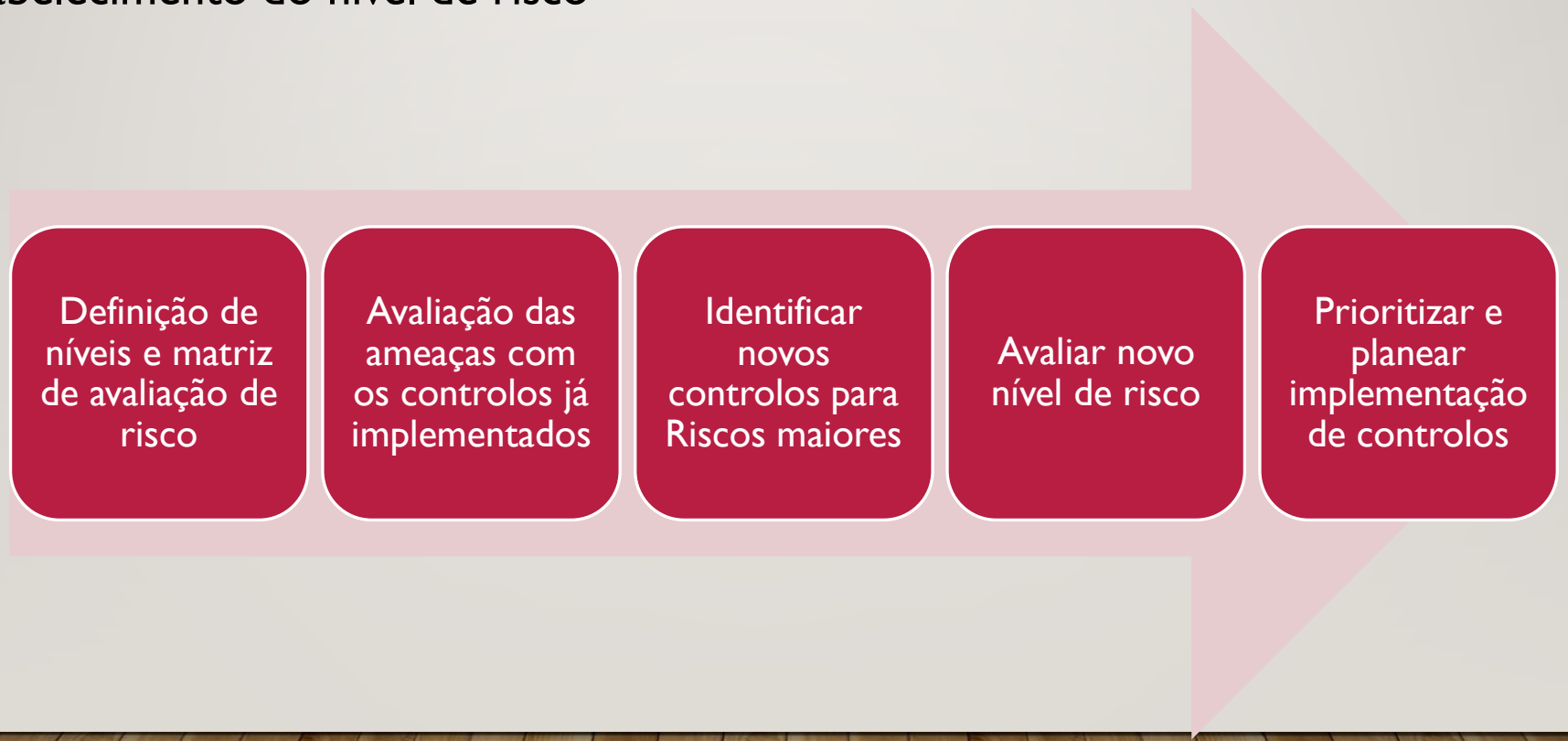
FRAP Session Agenda	Responsibility
• Introduction	
• Explain the FRAP process and cover definitions	• Owner + Facilitator
• Review scope statement	• Owner
• Review Visual Diagram	• Technical support
• Discuss definitions	• Facilitator

• 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

19 SESSÃO FRAAP

- Estabelecimento do nível de risco



20 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)	

21 SESSÃO FRAAP

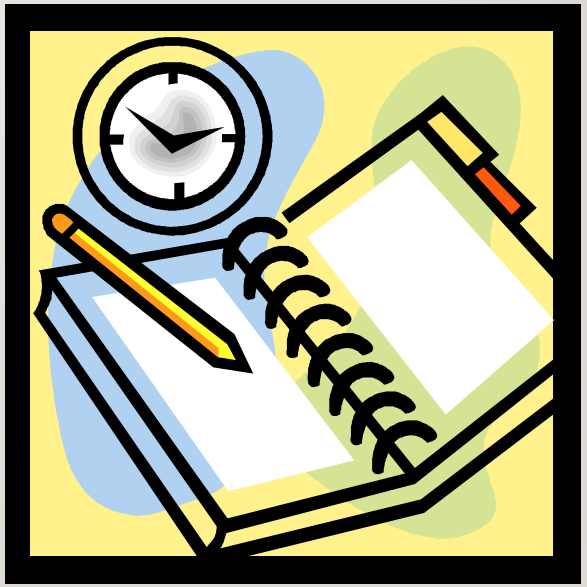
Definição de níveis e matriz de avaliação de risco → Avaliação das ameaças com os controlos já implementados → Identificar novos controlos para Riscos maiores → Avaliar novo nível de risco → Prioritizar e planear implementação de controlos

- 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		

22 SESSÃO FRAAP

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



23 EXERCÍCIO PRÁTICO

- Sala disposta em U
  - Caracterização de um sistema/processo
  - Condução de sessão FRAAP pelos alunos
    - Identificação de Ameaças/Vulnerabilidades para
      - Confidencialidade
      - Integridade
      - Disponibilidade
    - Identificação de possíveis controlos

24 AGENDA

- Revisão da aula anterior
  - Business Impact Analysis(BIA)
  - GAP Analisys
  - Definir uma Política de Segurança
- Processo de análise de risco FRAAP
- ➢ Identificação de ameaças e controlos para
  - a Cibersegurança
  - a Privacidade
  - Serviços na Cloud

25 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

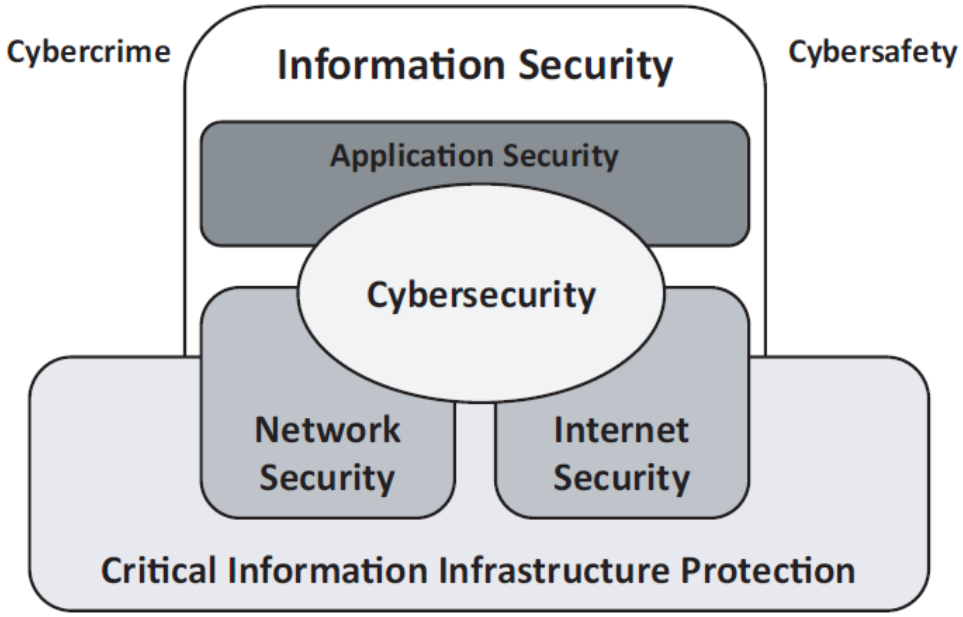


Figure 1 — Relationship between Cybersecurity and other security domains

26 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

30 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

31 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

32 SEGURANÇA DE SERVIÇOS NA CLOUD

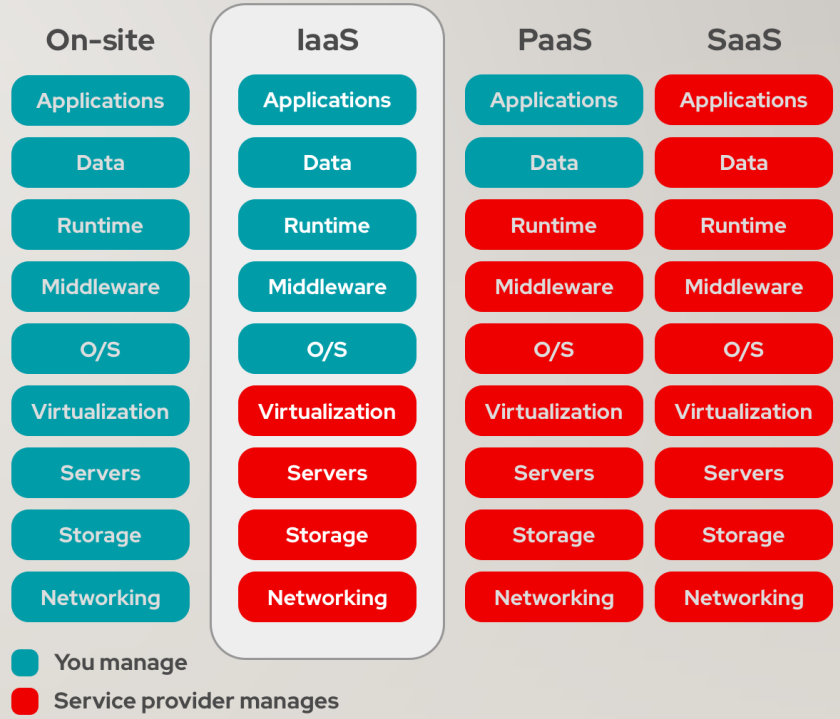
- Definidos requisitos em
  - ISO/IEC 27017 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

33 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)

34 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)



35 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.

36 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

37

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

FRAAP E AMEAÇAS E CONTROLOS ESPECÍFICOS DE SEGURANÇA

LUIS AMORIM

14 Mai 2022