Segurança e Gestão de Risco

2ºSem 2023/24

FRAAP

LUIS AMORIM

27 Abr 2024

AGENDA

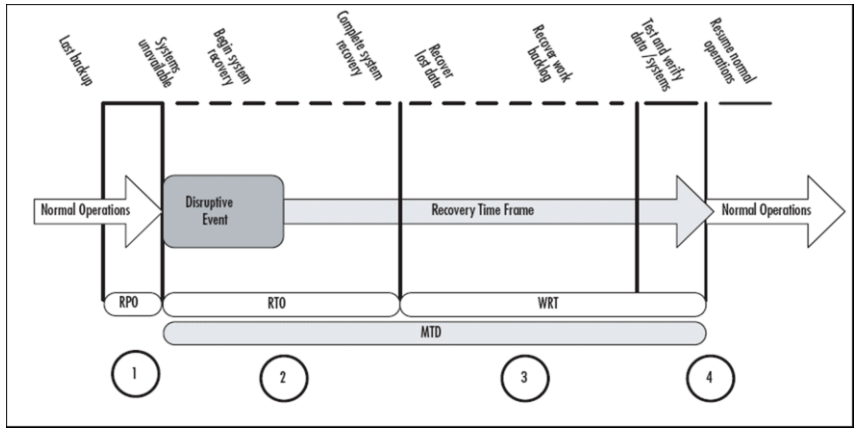
- Revisão da aula anterior
  - Business Impact Analysis(BIA)
  - GAP Analisys
  - Definir uma Política de Segurança
- FRAAP
  - Exercício prático
    - Pre-FRAAP
    - FRAAP

Síntese da Aula Anterior - Business Impact Analysis (BIA)

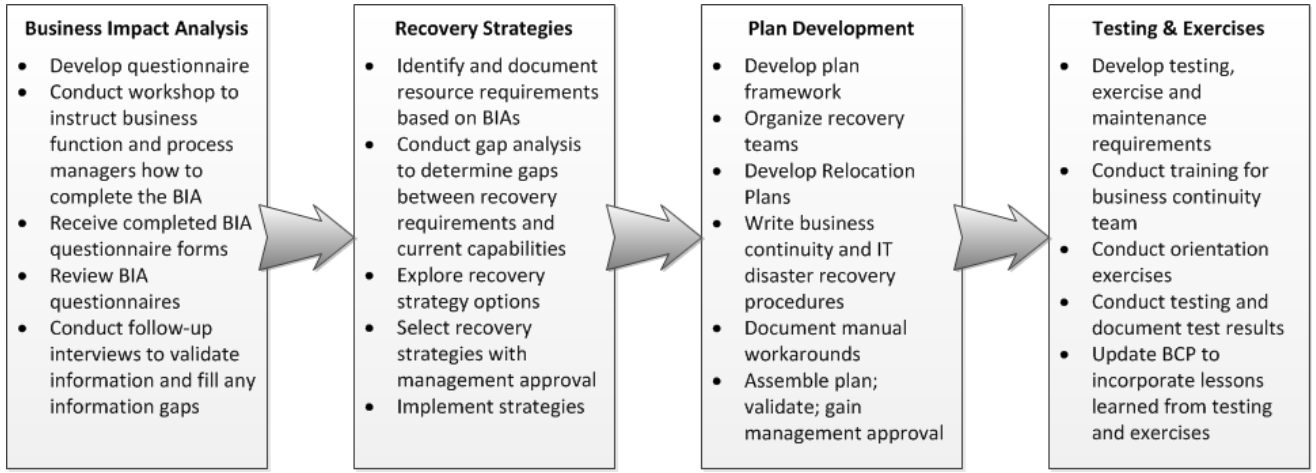
- Um processo de Business Impact Analysis pretende determinar os impactos que um incidente disruptivo tem na operação e na viabilidade dos processos core de negócio
- Implica antes
  - Determinar os processos core
  - Determinar quais são os principais recursos utilizados por esses processos
    - Aplicações;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

Síntese da Aula Anterior - Business Impact Analysis (BIA)

- Caraterizar os requisitos de recuperação
  - R P O = Recovery Point Objective R T O = Recovery Time Objective
  - W R T = Work Recovery Time
  - M T D = Maximum Tolerable Downtime



- Aplicar os resultados do BIA
  - Para estabelecer estratégias de recuperação



Síntese da Aula Anterior - 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 ___	

Síntese da Aula Anterior - Políticas 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

Síntese da Aula Anterior - Políticas 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.

Síntese da Aula Anterior - Políticas de Segurança

- Exemplo de

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.

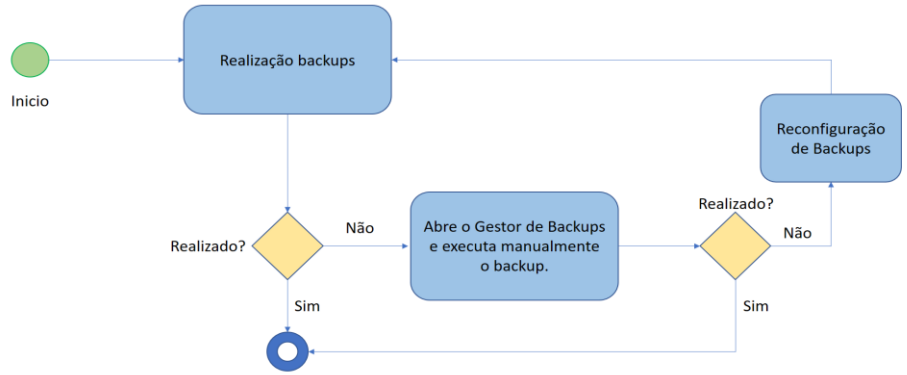
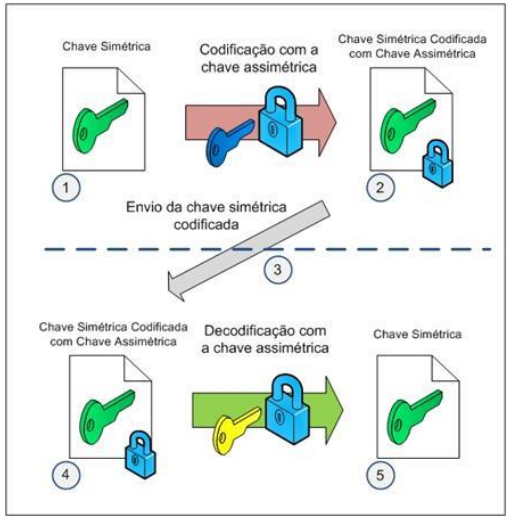
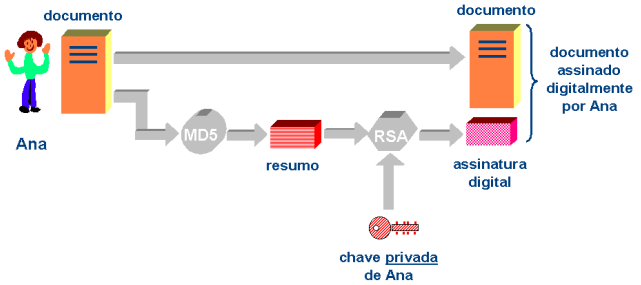


Figura 1 - Workflow de validação dos Backups

Síntese da Aula Anterior - Noções de criptografia

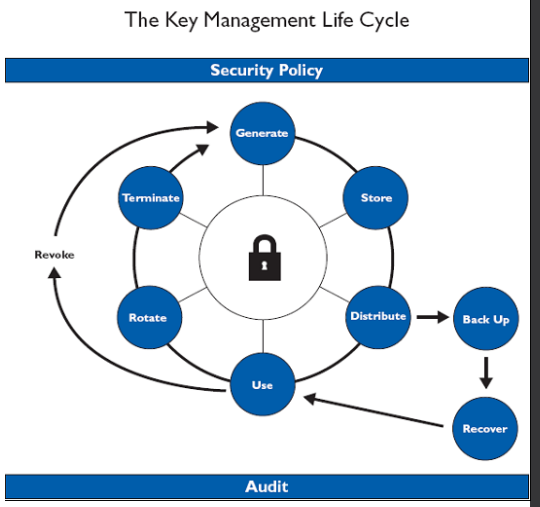
- Processos básicos de criptografia (Cifra e Decifra)
- Sistemas criptográficos simétricos
  - processamento mais rápido
- Sistemas criptográficos assimétricos
  - mais lento, mas mais seguro
- PKI – Public Key Infrastructure
- A Assinatura Digital



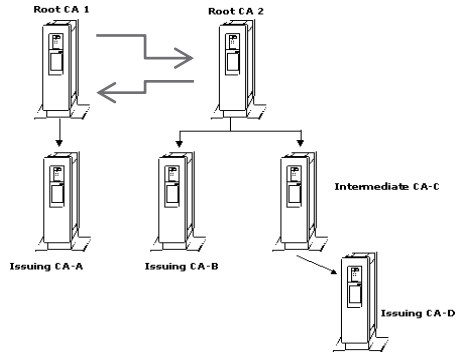


Síntese da Aula Anterior - Noções de criptografia

- Gestão de chaves
  - técnicas e procedimentos relacionados com o ciclo de vida das chaves criptográficas



- Relações de confiança entre CAs

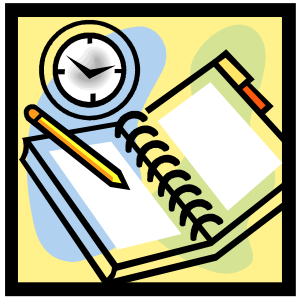


AGENDA

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

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 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)*

Processo de análise de Risco FRAAP

- FRAAP
  - Não deve durar mais que quatro horas
  - Envolver os elementos da equipa que
  - Deve ter a seguinte agenda
    - Introdução, preparada no Pre-FRAAP
    - Identificação de Ameaças e Vulnerabilidades
    - Identificação Controlos Existentes
    - Avaliar os níveis de risco (inerentes)
    - Identificar Riscos Residuais
    - Apresentação do Sumário da Reunião
  - Resultados esperados
    - Identificação das Ameaças
    - Identificação das Vulnerabilidades
    - Identificação dos Controlos Existentes
    - Caracterização dos Riscos Residuais

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

- 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)

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	

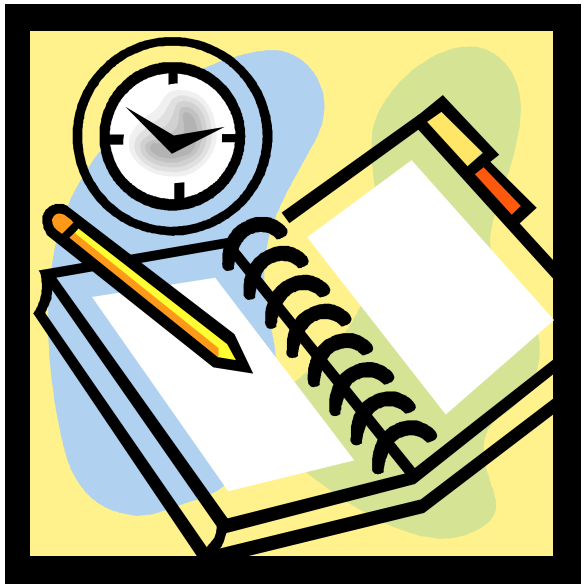
Sessão FRAAP

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

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

- Tratamento dos Riscos
  - Prioritizar 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 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 (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

Sumário Executivo

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

Sumário Executivo

Lista 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 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 tardiamente 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

Metodologias de Gestão de RiscoS

- Para suporte à Gestão de Risco pode ser utilizados referenciais como
  - ISO/IEC 27001 - Information security management systems – Requirements
  - ISO/IEC 27002 - Information technology- Security techniques - code of practice for information security management
  - ISO/IEC 27005 Information technology - Security techniques - Information security risk management
  - SP800-30 (NIST) - Risk Management Guide for Information Technology Systems
  - 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

Gestão de RiscoS

- Exercício Prático

Segurança e Gestão de Risco

2ºSem 2023/24

FRAAP

LUIS AMORIM

27 Abr 2024