Serviço de Hosting
STIC @ UA

Segurança e Gestão de Risco

Garcia Mateus

Gil Teixeira

Paulo Seixas

31/05/2023

Agenda

- A metodologia FRAAP

- Objetivos
  - O sistema
  - A equipa
  - Requisitos para a reunião FRAAP
  - Definições de princípio
  - Categorias de ameaças

- Mini-brainstorming

Metodologia FRAAP Facilitated Risk Analysis and Assessment Process

- Envolve a análise de 1 sistema/processo/plataforma de cada vez
- Permite uma redução do tempo de análise quando comparada a outras metodologias
- Utiliza um método qualitativo
- Promove a participação de toda a equipa no processo de avaliação e seleção de controlos

- Etapas do processo:
  - **Pre-FRAAP:** definir as bases do trabalho
  - **FRAAP**: Identificar: Riscos, Ameaças, Vulnerabilidades, Impactos e Controlos
  - **Post-FRAAP**: Análise de resultados e relatório final com a avaliação de riscos

Metodologia FRAAP Facilitated Risk Analysis and Assessment Process

- Definição do âmbito e objetivos
- Identificação de potenciais ameaças
- Avaliação e análise dos riscos
- Desenvolvimento de estratégias e controlos a aplicar
- Implementação de ações para tratamento dos riscos

Objetivos

Definir:

- Âmbito da avaliação
- Diagrama do Sistema
- A equipa (5-10 pessoas)
  - Pessoas com perfis e funções variadas
  - Facilitador, Escriba, Responsável do negócio, Gestor de projeto, Especialistas relacionados com o sistema
- Requisitos para a reunião FRAAP
  - Data/Hora:
  - Lugar:
- Definições de princípio
- Categorias de ameaças

Definições de princípio

- **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

Categorias de ameaças

- **Confidencialidade**
  - Roubo interno de informação
  - Acesso de pessoas não autorizadas a espaços restritos ou confidenciais
- **Integridade**
  - A perda de eletricidade pode corromper data
- **Disponibilidade**
  - Falha de eletricidade ou de hardware
  - Ataques de denial of service

    - **Outros**? (e.x. Performance ou Confiabilidade)

Mini-brainstorming

Obrigado