universidade de aveiro
theoria poiesis praxis

Relatório pré-FRAAP

Segurança e Gestão de Risco 23 | Sistema de Hosting - STIC

Grupo B: Garcia Mateus, Gil Teixeira, Paulo Seixas

1. Introdução

No âmbito da Unidade Curricular de Segurança e Gestão de Risco, foi proposto aos alunos, como forma de aplicar os conhecimentos obtidos em sala de aula, a realização de uma Avaliação de Riscos, seguindo a metodologia FRAAP, a um sistema real, nomeadamente ao serviço de hosting disponibilizado pelos STIC da Universidade de Aveiro.

Esta metodologia, desenvolvida por Thomas R. Peltier e que vem sendo aplicada e aprimorada nos últimos 15 anos, visa reduzir consideravelmente o tempo empregue neste tipo de avaliação, comparativamente com outras metodologias, apresentando uma boa relação custo-benefício. Promove o envolvimento de todos os atores que interagem com o sistema, sendo mesmo dirigida pelo responsável do negócio. Envolve a análise de 1 sistema de cada vez, e passa pelas seguintes etapas:

Pré-FRAAP ⟶ FRAAP ⟶ Post-FRAAP

Neste seguimento, serve o presente relatório para documentar os resultados obtidos na sessão Pré-FRAAP, realizada no passado dia 31/05, que o grupo teve a oportunidade de realizar junto dos STIC.

2. Sumário

A sessão Pré-FRAAP, teve uma duração de aproximadamente 1 hora (17h-18h, sendo que antes teve lugar uma sessão Pré-FRAAP conduzida por outro grupo relativamente a outro sistema) e permitiu definir as bases do trabalho. Contou com a presença dos responsáveis do sistema e teve como objetivo:

1. Definição do âmbito
2. Diagrama com a descrição/detalhe do sistema ou processo a avaliar
3. Identificação dos intervenientes/equipa a incluir no processo
4. Requisitos para a reunião FRAAP
5. Acordar definições de princípio
6. Mini-Brainstorming

2.1. Âmbito

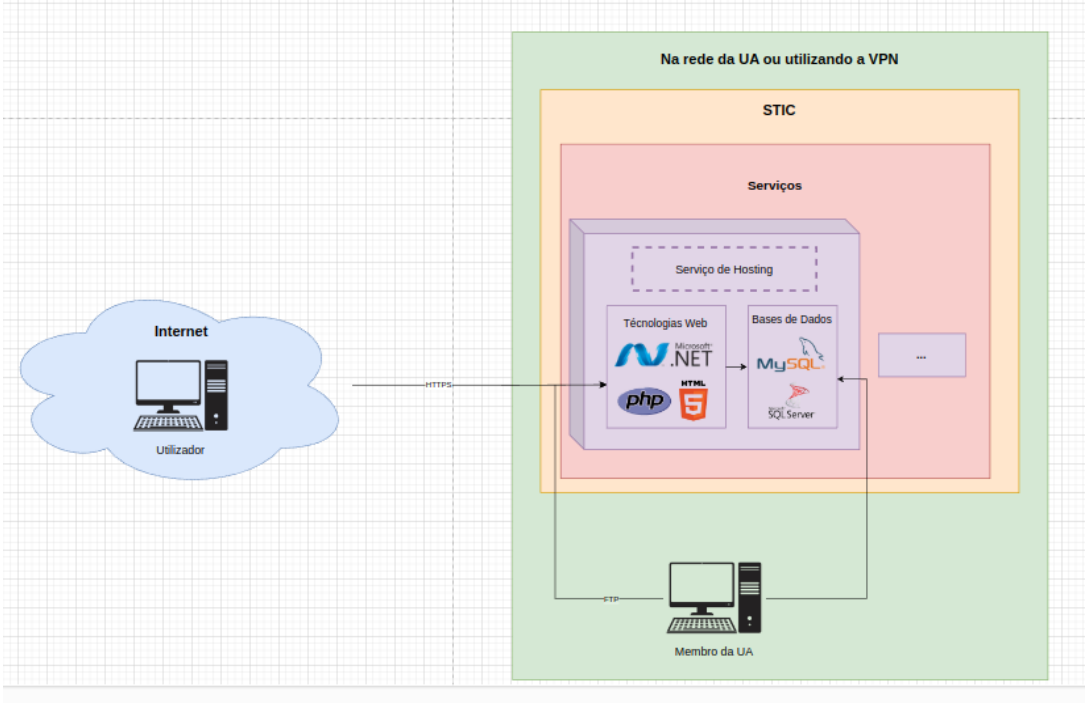
Foi definido, na sessão de pré-FRAAP, que a avaliação de riscos que o grupo irá realizar terá como alvo o sistema de hosting disponibilizado pelos STIC. Trata-se de um sistema que permite a diversas entidades (departamentos ou pessoas com vínculo à Universidade de Aveiro) alojar, principalmente, sites web.

2.2. Diagrama

O sistema oferece um diretório de ficheiros, onde o utilizador poderá colocar o seu código/projeto e, opcionalmente, uma base de dados. Esta poderá ser MySQL ou SQL Server, sendo que as tecnologias para desenvolvimento web suportadas vão desde php a .NET.

O sistema está desenhado numa infraestrutura *on-premise* e não oferece uma consola de gestão dos recursos, mas sim acesso ao diretório e bd acima referidos.

Durante a reunião foi pedido aos responsáveis pelo sistema o diagrama da plataforma, sendo que será devidamente incluído no relatório assim que nos seja facultado. Para já, deixamos uma visão muito alto nível, e do ponto de vista do utilizador, construída a partir daquilo que foi discutido.



2.3. Equipa

Consultores (Grupo C)	STIC
Facilitador: Paulo Seixas Escriba: Garcia Mateus Suporte: Gil Teixeira	Carlos Costa* - Project Manager/Owner Filipe Trancho* Alex Angélico José Ramalho Outros especialistas a convocar pelos responsáveis do projeto Utilizadores**

*Na impossibilidade de estar presente na sessão FRAAP; foi indicado que Alex teria o conhecimento e responsabilidade relativamente ao sistema, necessários para o efeito

**Foi pedido pelo grupo acesso ao sistema de hosting para ser possível, dentro do grupo de trabalho, obter experiência "*hands on*", do ponto de vista do utilizador.

2.4. Requisitos para a reunião FRAAP

A reunião de FRAAP ficou marcada para o dia 13/06, pelas 13h30, com uma duração estimada de 3 a 4 horas, tendo como limite máximo às 18h00. Esta terá lugar nos STIC, na mesma sala onde foi realizada a sessão pré-FRAAP.

2.5. Definições de princípio

Durante a sessão de FRAAP, foram discutidas e aceites as seguintes definições:

- **Ativo**: É um recurso com valor. Pode ser uma pessoa, um processo ou 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

Quanto à categorização das ameaças, foi aceite a utilização estandardizada dos 3 atributos para a segurança da informação: **Confidencialidade**, **Integridade** e **Disponibilidade**.

2.6. Mini-Brainstorming

Foi ainda possível, enquanto se inquiria por detalhes da arquitetura e funcionamento do sistema, identificar algumas ameaças a introduzir na reunião FRAAP, nomeadamente a não existência de redundância geográfica do *data center*, estando todo o sistema alojado num único local físico.