INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Ciberexercícios na Comunidade Académica

BRUNO DANIEL MONTE PEREIRA
Outubro de 2022

POLITÉCNICO
DO PORTO

Instituto Superior de Engenharia do Porto

Ciberexercícios na Comunidade Académica

CYBERLAB - CYBERSECURITY INNOVATION LAB FOR PUBLIC ADMINISTRATION

Bruno Daniel Monte Pereira

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Sistemas Computacionais

Orientador: Jorge Pinto Leite

Coorientador: Alexandre Gouveia

Júri:

Presidente:

Vogais:

Porto, outubro 2022

Resumo

Atualmente, uma grande parte dos serviços disponibilizados pela sociedade hoje em dia encontram-se acessíveis através de meios digitais. Apesar destes sistemas funcionarem partindo de um pressuposto que são seguros, a quantidade de tecnologias de informação utilizadas veio torná-los mais suscetíveis a ataques informáticos. Tendo em consideração a falta de ambientes de treino e de preparação dos profissionais de cibersegurança face a estes ataques, são necessárias medidas e ferramentas que forneçam soluções a esta problemática e apoiem os profissionais da área.

O projeto CyberLab visa implementar uma solução capaz de providenciar ambientes de treino em cenários simulados de ciberataques ajustados às necessidades da organização, com objetivo de formar e dar treino não só às equipas da área de segurança de informação, como também sensibilizar qualquer membro de uma organização face a estes ataques.

Este documento tem como objetivo fornecer uma contextualização dos principais conceitos do projeto e estado da arte face às soluções e estudos existentes relacionados com a temática de plataformas de treino e formação de segurança informática. O documento também visa proporcionar uma referência para planeamento dos ciberexercícios, apresentando exemplos e guias para a respetiva implementação.

Palavras-chave: Cibersegurança, ciberexercícios, certificação, treino, planeamento

Abstract

A large part of the services provided by society nowadays are accessible through digital means. Although these systems work on the assumption that they are secure, the amount of information technologies that these services use has made them more susceptible to cyberattacks. Considering the lack of training environments and preparation of the cybersecurity professionals regarding these attacks, more effective measures and tools are needed to provide solutions to this problem and support professionals in the area.

The CyberLab project aims to implement a solution capable of providing training environments in simulated scenarios of attacks that are adjusted to the needs of the organization, with the aim of providing training not only to the teams in the information security sector, but also with the purpose of making any member of an organization aware of these attacks.

This document has the intent to provide a contextualization of the main concepts of the project and the state of the art of the existing solutions and studies related to the subject of training platforms and cybersecurity training. This document also aims to provide a reference implementation and planning for cyber exercises, by providing examples and guideline for such endeavors.

Keywords: Cybersecurity, cyber exercises, certification, training, planning

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos e Símbolos

AP	*Administração Pública*
BT	*Blue Team*
CNCS	*Centro Nacional de Cibersegurança*
CR	*Client Requirements*
CSIRT	*Computer Security Incident Response Team*
CTF	*Capture the Flag*
EC	*Engineering Criteria*
ENSC	*Estratégia Nacional de Segurança do Ciberespaço*
IES	*Instituição de Ensino Superior*
ISO	*International Standards Organization*
NCD	*New Concept Development*
NIST	*National Institute of Standards and Technology*
RT	*Red Team*
SOC	*Security Operations Center*
TTP	*Táticas, Técnicas e Procedimentos*
UI	*User Interface*

1 Introdução

Este capítulo visa expor o enquadramento do projeto e do tema da tese, assim como apresentar os seus objetivos e contribuições.

1.1 Problema

Atualmente, uma grande parte dos serviços disponibilizados pela sociedade hoje em dia, quer sejam relativos à saúde, economia, ensino ou administração, encontram-se acessíveis através de meios digitais. Estes meios conseguem auxiliar os vários cidadãos de uma nação a realizar as suas atividades de uma forma mais acessível, informada e simplificada. Porém, com a contínua transformação digital presente nos dias de hoje, existe cada vez maior necessidade de acesso à Internet, o que tem acarretado diversos problemas de ciberataques. Apesar destes sistemas funcionarem partindo de um pressuposto que são seguros, a quantidade de tecnologias de informação utilizadas veio torná-los mais suscetíveis a ataques informáticos. Com vista a combater esta continuidade de ataques, várias diretivas a nível internacional, como a NIS[1], foram criadas e adotadas pelas diversas nações.

Contudo, perante esta realidade e a inerente divulgação de indicadores pelo Centro Nacional de Cibersegurança (CNCS), conclui-se haver uma falta de preparação e capacidade de resposta perante ciberataques das organizações, sistemas, e recursos humanos. Portugal ainda requer mais apoio e soluções inovadoras que permitam uma maior comunicação de incidentes e informações de riscos e ameaças entre instituições (CNCS - Centro Nacional de Ciber Segurança, 2019).

Uma das áreas onde este fenómeno está presente é a de Administração Pública e de Ensino Superior, nas quais a mão de obra não detém "*o know-how necessário para desenvolver internamente a atividade de cibersegurança*" (Universidade de Aveiro et al., 2019). Para além

[1] Ver capítulo 3.3 (pág. 15)

disso, os profissionais desta área não dispõem de "*modelos de aplicação direta, nem infraestruturas e/ou locais de experimentação de novas soluções, antes de as adquirirem ou colocarem no mercado*" (Universidade de Aveiro et al., 2019).

Pode-se inferir, igualmente, a falta de ambientes controlados de treino nos quais as equipas de segurança das organizações possam treinar cenários de ciberataque, exploração de vulnerabilidades, e formulação de cenários de treino, analisando tanto o ataque como a defesa apropriada (Universidade de Aveiro et al., 2019).

1.2 Descrição e Contexto do CyberLab

O *CyberLab – Cybersecurity Innovation Lab for Public Administration*, é uma iniciativa no âmbito do Sistema de Apoio à Modernização Administrativa (SAMA), fundada pela Agência para a Modernização Administrativa (AMA). Este projeto possui como objetivo principal a criação de uma infraestrutura na qual será possível a experimentação e treino de cenários e exercícios de cibersegurança. Tais exercícios contribuirão tanto para a melhoria na resposta a incidentes e ataques reais (já que, ao executar esses exercícios, os participantes treinam as suas capacidades de resposta e podem aprender novas técnicas), como também para a divulgação e promoção de boas práticas e ações de sensibilização no âmbito da segurança de informação.

A solução a desenvolver vem permitir aos membros do Consórcio otimizar os seus serviços e operações na área de segurança informática para com os *stakeholders* principais: membros da Administração Pública (AP) referentes aos setores de educação e ensino superior, membros da comunidade académica, e da sociedade que os rodeia. Esta iniciativa é conseguida através da operacionalização de uma plataforma adaptável às necessidades das Instituições de Ensino Superior (IES).

O Consórcio é composto por três IES: Universidade de Aveiro, Universidade do Porto, e Universidade de Trás-os-Montes e Alto Douro.

Para além da criação, execução, e análise dos exercícios que podem ser realizados, o CyberLab pretende suportar novos serviços e modelos de disseminação, prevenção e reação a ciberincidentes, estando, assim, alinhada com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

Esta infraestrutura é construída através de normas e recomendações de referência internacional, como as da *National Institute of Standards and Technology* (NIST) e da *Open Web Application Security Project* (OWASP), assim como com as recomendações por parte da *European Cyber Security Organisation* (ECSO), da *European Union Agency for Cybersecurity* (ENISA), e do CNCS.

1.3 Objetivos do CyberLab

O projeto CyberLab prevê, como objetivo principal, a criação de um laboratório de inovação e experimentação de soluções de cibersegurança adaptadas aos diferentes contextos da Administração Pública. Este laboratório deve fornecer um ambiente controlado para treino de resposta a incidentes e ciberataques, através de cenários práticos e exercícios de ataque e defesa no âmbito de cibersegurança, quer proativos quer reativos. Para além desta meta, destacam-se ainda os seguintes pontos como requisitos essenciais:

- Identificação, estudo e análise de modelos de treino e a sua adaptação a diferentes contextos organizacionais;
- Identificação e estudo de estratégias de disseminação de conhecimento e boas práticas de cibersegurança;
- Alinhamento do projeto com várias diretivas, recomendações e certificações internacionais (ISO 27001, NIST, OWASP, etc.);
- Disponibilização de um serviço online de discussão, partilha de conhecimento e de soluções inovadoras para a Administração Pública;
- Divulgação e promoção deste ambiente através de workshops, sessões de sensibilização, apresentações em fóruns e redes nacionais e internacionais da área da cibersegurança e da administração pública;
- Contribuição para a Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023.

1.4 Contribuições

O CyberLab auxilia a AP tanto a nível interno como externo. Tem vantagens a nível interno, já que permite aumentar a capacitação e eficiência na resposta a incidentes de cibersegurança na comunidade envolvida na administração local, central, e entidades do setor empresarial. Tem vantagens também a nível externo, já que o aumento na melhoria destes serviços proporciona uma mais-valia para a sociedade e para os seus cidadãos.

Desta forma, as IES da Universidade do Porto, Universidade de Aveiro, e Universidade de Trás-os-Montes e Alto Douro, atuaram como pilotos no projeto, tornando-se, assim, instituições de referência no mesmo, através da adoção de boas práticas e resultados obtidos, em outras instituições nacionais. É de notar que estas IES detêm a oportunidade de oferecer estes serviços de treino a empresas externas, de forma que essas entidades possam também capacitar os seus trabalhadores para uma melhor resposta a incidentes.

1.5 Objetivos da Dissertação

Como a realização deste documento integra-se no âmbito da disciplina de Tese/Dissertação/Estágio do Mestrado de Engenharia Informática (TMDEI) do Instituto Superior

de Engenharia do Porto, é necessário especificar quais os objetivos propostos do trabalho realizado durante o respetivo ano letivo que visam ser cumprido e apresentados na atual dissertação.

O plano no início do ano letivo seria cumprir com os objetivos propostos e normas planeadas pelo projeto CyberLab. Porém, a situação atual é de que as instalações da solução nas máquinas das universidades ainda não aconteceram, devido a atrasos no processo de contratação de soluções de empresas externas. Devido a este facto, não será possível mostrar resultados concretos da criação de ciberexercícios em ambiente de laboratório de inovação e experimentação destes exercícios.

Com isto, ponderou-se uma alternativa para apresentar resultados concretos para comprovar o desenvolvimento da dissertação. O objetivo do trabalho consiste em apresentar normas e diretivas de como construir e elaborar exercícios de cibersegurança adaptados ao contexto da IES. Desta forma, o trabalho estará orientado para, quando no futuro as soluções de empresas externas estiverem instaladas na universidade, seja mais fácil implementar os exercícios que foram desenhados. Assim, o presente trabalho tem como objetivo dar a conhecer ao leitor umas linhas de guia para como realizar e preparar um exercício, apresentando dois exemplos de ciberexercícios detalhados. Também se realizou uma segunda análise na componente de Experimentação e Avaliação baseado em como usar os resultados das pontuações dos ciberexercícios e realizar testes estatísticos.

1.6 Estrutura do Documento

Este documento está dividido em oito capítulos.

O capítulo 1 apresenta o contexto em que o projeto se insere, a motivação da sua criação, os seus objetivos e contributos para as partes interessadas.

Tendo em conta um dos objetivos principais do projeto, o segundo capítulo atende à contextualização de ciberexercícios, apresentando o seu ciclo de vida, como são organizados e quais a principais equipas envolventes. Também são explicados alguns dos tipos de exercícios que se prevê implementar na solução e as suas características.

O capítulo 3 contextualiza o leitor perante as várias *frameworks* e diretivas que certificam a segurança de informação de um sistema ou de uma organização. Os modelos e normas demonstrados neste capítulo são os previstos a serem utilizados no contexto do CyberLab.

O capítulo 4 referencia a análise de valor do projeto, percorrendo várias vertentes tais como a justificação da ideia da solução, o valor que se pretende trazer aos *stakeholders,* quais os requisitos e fatores de engenharia mais importantes e como selecionar a melhor alternativa de software para o efeito desejado.

No capítulo 5 é apresentada uma compilação de informação de vários guiões de planeamento de ciberexercícios, de maneira a instruir e orientar para esta prática.

Este capítulo é complementado com o capítulo 6, no qual estão expostos dois ciberexercícios de exemplos, construídos com os conhecimentos colecionados no capítulo 5.

Para planeamento das metodologias de avaliação dos exercícios, demonstrou-se no capítulo 7 quais as hipóteses de investigação, a metodologia para as, quais as principais métricas e variáveis que é possível compilar, e como medi-las através de testes estatísticos.

Finalmente, é apresentado no capítulo 8 a conclusão do conteúdo do documento, assim como quais foram as principais limitações encontradas e o planeamento do trabalho futuro.

2 Ciberexercícios

O projeto CyberLab tem como um dos principais requisitos a capacidade de criar e realizar cenários e exercícios de cibersegurança. Como tal, é importante perceber qual é a estrutura de um ciberexercício, qual o seu ciclo de vida, e que tipos de exercícios existem. Este conhecimento será usado aquando da implementação da solução, garantindo que esta cumpre com os padrões já existentes. Este capítulo visa realizar um resumo da contextualização dos ciberexercícios, no qual será exposto o ciclo de vida dos mesmo e alguns dos tipos de cenários mais relevantes para o contexto do projeto: o Cyber Range, o Capture the Flag (CTF), e o Threat Hunting.

2.1 Ciclo de Vida dos Exercícios

Um exercício de cibersegurança, quando usado para simular situações e cenários reais, pode ser dividido em três principais fases: a de planeamento, a de implementação, e a de avaliação:

2.1.1 Fase de Planeamento

Nesta fase define-se o propósito do exercício e as suas limitações (Nina Wilhelmson, 2011). É através do exercício que determinados objetivos pedagógicos são atingidos e, através destes, é possível idealizar os parâmetros do mesmo (Karjalainen et al., 2019). Cada organização pode utilizar as ferramentas que achar relevantes para o planeamento do cenário de maneira que os participantes consigam colocar as suas habilidades à prova (Şeker, 2019). É também importante aqui definir as métricas de avaliação do desempenho do participante (Nina Wilhelmson, 2011).

Nesta fase é também fulcral ter em conta que as equipas participantes no exercício podem não usar a melhor estratégia para o resolver, e cabe à "equipa branca", os moderadores, saber orientá-los na direção correta caso haja necessidade. É importante também ter noção da dimensão do exercício, já que quando estes são feitos em grande escala, existem várias

limitações que devem ser mitigadas para o bom planeamento, como o orçamento para esse treino, a disponibilidade das pessoas organizadoras, tempo de planeamento, entre outros (Karjalainen et al., 2019).

2.1.2 Fase de Implementação

É nesta fase que decorre a realização do exercício, levando a cabo os objetivos definidos. No decorrer do mesmo, cabe à "equipa branca" a responsabilidade de manter uma observação constante do exercício. É importante ter em conta que nesta fase pode haver necessidade de ajustar os parâmetros de um exercício para corresponder melhor aos objetivos definidos na primeira fase (Karjalainen et al., 2019). É de salientar que as regras de cada exercício a ser realizado são normalmente transmitidas aos participantes antes do início do mesmo, de maneira que as equipas possam planear uma estratégia ou adquirir as ferramentas necessárias para a sua concretização. Porém, isto pode variar de acordo com os objetivos do exercício (Şeker, 2019).

Tipicamente, existem várias equipas que são envolvidas num exercício. Para efeitos de explicação das mesmas neste documento, usar-se-á, como exemplo, um cenário que envolve uma equipa que ataca e outra que defende. Nesta tipologia de exercícios existem duas principais equipas: a azul (defesa) e a vermelha (ataque). A equipa azul tem como objetivo defender contra qualquer ameaça provocada pela equipa atacante no sistema virtual e simulado especificado. Tem também como objetivo mitigar qualquer fuga de informação ou brecha à rede. É importante que estes participantes tenham conhecimento das legislações e normas atualmente impostas, já que, apesar de se encontrarem num ambiente simulado, não devem praticar numa ilegalidade (por exemplo, violação de privacidade dos dados). No outro lado do espetro, encontra-se a equipa vermelha, cujo objetivo é explorar quaisquer vulnerabilidades na equipa azul, de acordo com o cenário que foi fornecido. Qualquer ataque bem-sucedido influencia a pontuação, descontando pontos na equipa azul.

Para além destas equipas, existem ainda mais quatro: a verde, branca, amarela, e a dourada. A equipa verde é responsável por gerir as redes e infraestruturas e sistemas de virtualização do cenário, de modo que estejam constantemente a funcionar. A equipa branca, como mencionado previamente, tem o propósito de definir os requisitos, objetivos, e regras de cada exercício na fase de planeamento. Na fase de execução, tem um papel de analisar e controlar as diferentes fases do exercício, proporcionando especial atenção ao desempenho da equipa vermelha, e controlar a pontuação. Dentro da equipa branca pode haver uma subequipa: a equipa dourada, cujo objetivo é simular utilizadores do sistema inexperientes, vulneráveis a técnicas de engenharia social, os quais a equipa azul terá de dar especial atenção. Finalmente, existe a equipa amarela, cujo objetivo é disseminar informação acerca das ocorrências nos exercícios, primeiro à equipa branca e depois aos restantes participantes. Os documentos que relatam as atividades da equipa azul e vermelha são das suas principais fontes de informação (Şeker, 2019).

2.1.3 Fase de Avaliação

A terceira e última fase referem-se ao feedback do exercício aos participantes. É de salientar a importância de haver um período de Q&A (perguntas e respostas) e de explicação da realização e abordagem correta do exercício (Karjalainen et al., 2019). Apesar de haver a possibilidade de incluir pontuação associada ao exercício, muitos organizadores defendem que não é esse o principal foco do desafio, colocando com maior grau de relevância a sensibilização às ciberameaças e à melhoria das capacidades dos participantes (Şeker, 2019). Consoante os escopos do exercício, vários estudos podem ser realizados para verificar o sucesso dos cenários que foram levados a cabo. Podem ser incorporados metodologias de investigação para avaliar o comportamento social dos participantes. Isto leva a questões como: "Porquê que realizaram estes passos?"; "Porque é que não consideraram um determinado componente uma ameaça?"; "Porque não conseguiram identificar uma determinada vulnerabilidade?"; entre outras (Granåsen and Andersson, 2016). Tais estudos tem a capacidade de ajudar a entender como decorreu o ciberexercício, avaliando: a sua dificuldade; o estado das equipas perante os problemas de cibersegurança propostos; se o exercício se relaciona com vulnerabilidades atuais ou mais tendenciosas nos dias de hoje; ou mesmo se o exercício conseguiu simular de forma precisa uma situação real (Ošlejšek et al., 2018). A título de exemplo, tal aconteceu num caso de estudo pela NATO Cooperative Cyber Defence Centre of Excellence e pela Swedish National Defence College, no qual a prestação e desempenho de várias equipas foram estudados, provando que é possível criar cenários minimamente realistas. Nestes cenários foi possível criar uma boa estratégia e comunicação entre os membros de cada equipa. Comprovou-se que os melhores resultados de vulnerabilidades descobertas, correção das mesmas e elaboração de relatórios dependem imenso da estratégia usada pelas equipas, onde as poucas mudanças de organização das equipas, a disciplina em manter a estratégia de ação e de trabalho para a concretização dos objetivos, e melhores qualificações e experiência individuais levam a melhores resultados no geral. A equipa vencedora mostrou uma abordagem mais proativa nas suas defesas, em vez de reativa, o que auxiliou na sua classificação (Granåsen and Andersson, 2016).

2.2 Tipologia dos cenários

A plataforma do CyberLab vem permitir a criação de vários tipos de exercícios e/ou cenários para diversos propósitos, desde a obtenção de maior conhecimento na área de cibersegurança, até a simulação de sistemas vulneráveis para competições e eventos de ataque e defesa. Assim, serão aqui listados alguns dos tipos de cenários possíveis de serem criados na plataforma:

2.2.1 Cyber Range

Um Cyber Range é um ambiente controlado e interativo que permite aos profissionais de cibersegurança aprender a detetar e mitigar incidentes de cibersegurança. Através de sistemas de monotorização de progresso e desempenho, é possível avaliar o utilizador de acordo com as

suas aptidões em resolver o incidente em questão. Assim, um Cyber Range deve ser capaz de permitir que um membro da organização do exercício possa orquestrar e configurar o ambiente para incluir uma determinada brecha de segurança, de modo que um participante possa aplicar as suas técnicas de defesa para a resolução do ataque. Estes ambientes são infraestruturas complexas e podem ser compostas de várias máquinas virtuais e/ou físicas (Taylor, 2021).

Como referido, o principal valor destes cenários é permitir que os utilizadores não só melhorem as suas aptidões de cibersegurança, mas também fornecer ferramentas de pesquisa e testagem de segurança. Para além disto, também permitem uma valiosa ferramenta para garantir a continuidade de operações (COOP) de um determinado software da empresa, permitindo uma avaliação de risco e segurança em pré-produção do mesmo aquando de uma nova atualização (CyberExer, 2021).

É de salientar que este género particular de exercícios é útil para melhorar o funcionamento de uma equipa azul. Não só os Cyber Ranges conseguem mostrar métricas e *Key Performance Indicators* (KPI) de desempenho de quem nele participa como também ajuda a melhorar as capacidades de qualquer colaborador de um *Security Operations Center* (SOC). A capacidade de replicar ataques sofisticados é benéfico para que pessoas com ou sem experiência na área consigam entender os ataques que acontecem em situações reais e melhorar a cultura de cibersegurança de uma organização (Henry, 2019).

2.2.2 Capture the Flag (CTF)

Uma competição CTF é um evento no qual participantes (podendo ser de participação individual ou por equipas) competem entre si para obter o maior número de *flags* (pequenas sequências de caracteres, podendo conter uma mensagem legível ou não) durante o tempo da prova de maneira a adquirir mais pontos que os adversários. Estas competições são em certas ocasiões o ponto de entrada na área de cibersegurança, já que permitem a realização de pequenas simulações ou cenários de diferentes níveis de dificuldade, nos quais os participantes deverão aplicar os seus conhecimentos de segurança informática ou ciência de computadores. (2021)

Tais competições são benéficas para testar as capacidades de ataque de uma equipa e aprender novas capacidades ou técnicas na concretização nos desafios. A componente competitiva e dinâmica ajuda a que os participantes desenvolvam estratégias de comunicação e trabalho em equipa para conseguir cumprir com os objetivos. Como todos os exercícios são em ambientes simulados e não existe um risco elevado de comprometimento de máquinas ou software reais, as equipas e os seus membros acabam por ter uma motivação diferente na sua realização (HackEdu), focando-se mais na melhoria de capacidades individuais, aprendizagem de novas técnicas e, também, partilha de informações e criação de ligações entre os participantes.

Cada exercício pode ser de várias categorias. Abaixo estão listados apenas alguns exemplos, já que podem existir outras:

- **Forensics:** Os participantes devem utilizar ferramentas para investigar um determinado problema ou recuperar algo de um ficheiro, imagem, tráfego, etc. Nesta categoria pertencem os exercícios de captura de tráfego, operações em ficheiros e esteganografia;
- **Cryptography:** Nesta categoria, os participantes têm de decifrar uma mensagem encriptada usando diversas metodologias e ferramentas. Dentro destes desafios podem fazer parte diversas cifras, *hashes* ou codificações;
- **Exploitation:** Nestes desafios, os participantes têm de explorar uma vulnerabilidade num sistema controlado e construído para esse propósito. Existem inúmeras vulnerabilidades possíveis, tais como SQL Injection, XSS, Cross Site Request Forgery ou Command Injection;
- **Reverse Engineering:** Nesta categoria, os participantes têm de converter um programa compilado para código, através de um descompilador.
- **OSINT:** Estes desafios envolvem *Open Source Intelligence* (OSINT), nos quais os participantes deverão procurar informações sobre o contexto da prova em materiais e fontes abertas e públicas online.

2.2.3 Threat Hunting

Threat Hunting é a prática de procurar ciberameaças num sistema. Tendo em conta as várias fases de um ciberataque, esta prática tem maior predominância quando um atacante se instala num sistema ou coleciona dados ou conteúdo confidencial que lhes permite mover lateralmente nesse sistema. Desta forma, quando um utilizador trabalha num cenário simulado e controlado de Threat Hunting, este deve assumir que o mesmo já se encontra comprometido. Através de informação de atividades incomuns ao funcionamento do sistema, é possível investigar o problema e formular uma hipótese de onde e como o ataque está a ser realizado. Esta prática combina tanto inteligência e análise humana, como várias tecnologias e indicadores para detetar e resolver a ameaça (Taschler, 2021).

Depois de formular essa hipótese, poder-se-á optar por uma abordagem estruturada, não-estruturada ou situacional (IBM).

- **Estruturada:** Esta abordagem é baseada no indicador de ataque (IOA) e nas táticas, técnicas e procedimentos (TTP) do atacante, tornando-se mais fácil identificar o ator. Esta abordagem utiliza a *framework MITRE Adversary Tactics Techniques and Common Knowledge (ATT&CK)*;
- **Não-estruturada:** Esta abordagem baseia-se numa causa e num indicador de compromisso (IoC). Esta causa pode auxiliar o "caçador" a procurar padrões que o guiem a entender as motivações, *modus operandi,* e identidade do atacante;
- **Situacional:** Esta abordagem baseia-se numa gestão de risco interna ou tendências de análise de vulnerabilidade que permitem associar um comportamento a uma causa e a um TTP.

3 Normas e Referências de Segurança

O CyberLab compromete-se a dar sustentabilidade às estratégias nacionais e internacionais de cibersegurança, através de recomendações e *frameworks*. Não só isso melhora a qualidade do serviço e a sua arquitetura, como também fornece uma garantia de qualidade ao cliente. De seguida, estão listadas e apresentadas algumas das normas que o CyberLab prevê que sejam usadas na solução.

3.1 NIST NICE Cybersecurity Workforce Framework

Esta *framework*, publicada pela NIST, descreve a Framework de Força de Trabalho para Cibersegurança, sendo uma referência para descrever as qualidades necessárias para uma determinada função numa área. A *framework* resume-se a uma maneira de dividir e categorizar o trabalho necessário que se exige de um colaborador:

- **Tarefa:** Uma atividade que está direcionada com o cumprimento de um objetivo;
- **Conhecimento:** Um conjunto de conceitos provenientes da memória;
- **Habilidade:** A capacidade de realizar uma ação;
- **Competência:** Um mecanismo para a organização avaliar os colaboradores.

Com esta divisão, é possível criar um sistema que descreve uma *taskforce*, composta por várias tarefas, onde cada uma tem de ser executada por alguém com determinado conhecimento e habilidade. Desta forma, uma organização pode facilmente criar uma competência para uma determinada função, na qual o colaborador, de modo a ser aceite para desempenhá-la, deverá possuir determinados conhecimentos e habilidades (em inglês, Knowledge and Skills (K&S)) de modo a executar uma ou mais tarefas dessa função com sucesso (NIST - National Institute of Standards and Technology, 2020).

No contexto do CyberLab, esta ferramenta pode ser utilizada para descrever que competências um utilizador deve ter para realizar um exercício, ou quais competências pode adquirir através de uma ação de formação.

3.2 NIST Framework

A *framework* da NIST oferece uma linguagem comum para perceber e gerir o risco de cibersegurança dentro de uma organização. Serve não só para alinhar políticas e abordagens tecnológicas dentro da mesma, como também para priorizar ações para um determinado risco de segurança informática.

O núcleo da *framework* oferece uma lista de atividades associadas a um objetivo de cibersegurança, na qual os grupos de trabalho podem-se guiar para gerir o risco. Existem 5 funções: identificar, proteger, detetar, responder e recuperar. Estas funções servem para auxiliar a organizar as tarefas de cibersegurança para várias categorias personalizadas pelo utilizador.

Para além disso, existe o conceito de patamares de consciência nos quais uma organização pode ser considerada. Estes níveis consideram o quão ela está preparada a lidar com incidentes, práticas de gestão de risco, práticas de partilha de informação, etc. São estes níveis:

1. **Parcial:** não existe muita conscientização de cibersegurança e a resposta a incidentes é geralmente reativa e *ad hoc*;
2. **Informada do risco:** tem alguma sensibilização para os riscos, mas é muito limitada em algumas áreas, como a partilha de informação e a priorização da segurança nos sistemas;
3. **Repetível:** organização bastante formalizada e consciente dos riscos e das práticas;
4. **Adaptável:** organização adapta os seus processos de segurança a experiências passadas e o comportamento é constantemente monitorizado.

É expectável que sejam criadas hierarquias entre os colaboradores de uma organização para transmitir, planear e executar as operações, onde a informação e comunicação são valorizadas para que a estratégia executiva ao nível operacional seja fluída. A organização deve seguir uma sequência de boas práticas em como usar esta *framework*, passando por fases tais como: a priorização e definição do âmbito; a orientação e o planeamento; a criação do perfil atual (onde se especifica quais as categorias dos *outcomes* que estão a ser trabalhados atualmente); a realização uma avaliação de risco; criação um perfil alvo (onde se especificam os *outcomes* desejados a atingir); identificação das falhas que não permitem atingir esse objetivo alvo e criação e organização de um plano para colmatar essas falhas; e, finalmente, implementação do plano de ação (NIST - National Institute of Standards and Technology, 2018).

3.3 Diretiva NIS

A diretiva NIS é uma parte da legislação europeia para a cibersegurança, primeiramente adotada em 2016. O seu objetivo é coordenar os vários serviços de cibersegurança dos estados-membros para trabalharem cooperativamente para a melhoria do ciberespaço (ENISA - European Union Agency for CyberSecurity). Alguns dos objetivos desta diretiva são (European Union, 2016):

- Criação de um grupo de cooperação para suportar as várias estratégias de troca de informação entre todos os Estados Membros;
- Criação de uma rede de equipas de resposta a incidentes (CSIRT's) para contribuir para o desenvolvimento de melhor capacidade de resposta a incidentes e reportagem dos mesmos;
- Supervisão da segurança dos setores críticos de cada estado-membro (energia, transporte, saúde, canalização, defesa, bancos, etc.).

Esta diretiva tem sido alvo de revisões ao longo do tempo, sendo que em 2020 a Comissão Europeia e o Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança apresentaram uma revisão e novas medidas para aumentar a capacitação europeia para resposta a incidentes, resiliência contra ataques informáticos, e benefícios aos cidadãos. Nesse mesmo ano, a Comissão Europeia recebeu a confirmação de que todos os estados-membros abrangeram os objetivos da diretiva nas suas legislações nacionais. Porém, isto não provou ser o suficiente para a concretização dos objetivos definidos no contexto da diretiva. Depois de avaliada e estudada a sua aplicabilidade e relevância, foi concluído que os critérios dos serviços críticos nacionais não estavam suficientemente claros, pelo que alguns não eram abrangidos pela diretiva e, como tal, não tinha a obrigação de implementar estas medidas ou relatar problemas à Comissão Europeia. Para além disso, comprovou-se que existia muita discrepância nos requisitos de reportagem e resposta de incidentes a tais serviços por parte das equipas nacionais. Finalmente, concluiu-se que não havia níveis satisfatórios de partilha de informação na rede, principalmente entre empresas privadas (Negreiro, 2021).

Devido a estas razões, a diretiva NIS 2 veio tentar solucionar este problema. Esta proposta foi oficialmente apresentada em abril de 2021 e tenta, entre outros objetivos: aumentar os níveis de supervisionamento das equipas de segurança nacionais; implementar novas medidas de segurança a várias cadeias de distribuição; e aumentar o alcance das várias medidas de segurança de modo a cobrir mais organizações e empresas, tanto públicas como privadas. De uma forma geral, vem aumentar a exigência de regulamentações de segurança aos vários setores críticos e equipas nacionais de resposta a incidentes (Achiaga, 2022).

3.4 MITRE ATT&CK

A *MITRE Adversarial Tactics, Techniques, and Common Knowledge* (MITRE ATT&CK) é uma *framework* que pretende refletir os vários comportamentos e perfis de um atacante, assim como refletir os vários ciclos de vida de um ataque. Este modelo auxilia na categorização e taxonomia de várias ações e como defender delas (McAfee).

Os principais componentes do modelo são as táticas (objetivos dos atacantes), e técnicas (como é que o atacante atinge esses objetivos). Ao aplicar o MITRE ATT&CK num contexto ou ambiente Windows, Linux, MacOS, AWS, Azure, entre outros, é possível ordenar estas táticas e técnicas numa matriz adaptada aos vários ambientes, onde, para cada tática, existem várias técnicas possíveis. Um exemplo desta matriz poderá ser consultado no Anexo A (McAfee).

Este modelo auxilia no desenvolvimento do CyberLab devido à profundidade que aborda cada fase do ataque, de onde é possível emular cenários de teste tendo em conta o comportamento do adversário. É um modelo útil na organização de um plano de defesa e predizer padrões de ataque, assistindo, como referido anteriormente, em cenários de Threat Hunting.

3.5 Família ISO 27000

A International Standards Organization (ISO) é uma organização não-governamental que cria normas de negócio para facilitar a coordenação empresarial e certificação de serviços. Estes objetivos são cumpridos através dos vários *standards* utilizados em vários domínios (segurança, ambiente, saúde, etc.), que ajudam não só a certificar um serviço ou produto, como proteger os seus clientes (Behaviour, 2017).

Das várias normas existentes, destaca-se, no âmbito do projeto CyberLab, a família 27000, que cobre a área de segurança informática. Apenas a ISO 27001 é considerado um *standard* certificado, pelo que todas as outras normas são apenas guias para implementação dos serviços. Algumas destas normas são:

- **ISO 27002:** Guia de boas práticas para gestão de sistemas de gestão de informação;
- **ISO 27005:** Guia para implementação de uma gestão de avaliação de risco, de acordo com os processos e modelos especificados na norma ISO 27001;
- **ISO 27007:** Guia para auditoria de um sistema de informação;
- **ISO 27011:** Guia para aplicação da ISO 27002 na área de telecomunicações.

3.5.1 ISO 27001

A ISO 27001 é uma norma que estabelece requisitos para a implementação, operacionalização, monotorização e revisão de um Sistema de Gestão de Segurança de Informação (SGSI) (Behaviour, 2017). Este padrão tem sido iterativamente melhorado ao longo dos anos, desde a sua conceção em 1992, a partir de um documento estabelecido pelo governo britânico. É

expectável que qualquer organização que utilize esta norma consiga mitigar e gerir de forma correta os riscos da segurança de informação e todos os seus sistemas relevantes a esta área. A ISO 27001 abrange todos os aspetos que possam comprometer a segurança informática de uma organização, desde as telecomunicações, proteções físicas, dados pessoais, continuidade do negócio, entre outros (Integrity, 2022).

Em modos gerais, a organização deve primeiro compreender de forma clara o motivo para escolher implementar esta norma. Deve traçar objetivos e perceber se a gestão de topo consegue comprometer-se a assegurar que a estratégia para a melhoria da segurança organizacional e dos seus sistemas seja levado a cabo com eficácia e com o apoio necessário. Depois de planear como irá integrar e implementar as ações nos processos do sistema de forma a evitar efeitos secundários indesejáveis, deverá fazer tanto uma análise de risco à organização e elaborar uma política de segurança (Qualidade, 2013).

De seguida, deve ser elaborado um plano de mitigação dos incidentes, de maneira a manter a continuidade do negócio e perceber que ações realizar em caso de ataque, de incidente, ou de desastre. Depois de definição destas normas, documentos e planos, torna-se essencial o treino dos recursos humanos e gradual implementação destas medidas nos processos da organização. Todos estes processos devem ser sujeitos a melhorias constantes e auditorias tanto internas como externas para um constante investimento nos processos de segurança da organização (Kosutic).

4 Análise de Valor

O projeto consiste na criação de uma plataforma capaz de criar exercícios e cenários de cibersegurança acessíveis a diversas pessoas de uma organização, criar, testar e analisar modelos operacionais às estruturas da organização, e criar uma pareceria entre as várias instituições do consórcio. Para além disso, o projeto visa um produto com alta credibilidade, já que aposta no uso de *frameworks* e recomendações internacionais e na disseminação e aplicação de boas práticas.

Este capítulo irá retratar o valor do CyberLab, através de modelos como o CANVAS, o *New Concept Development*, e o SWOT. Irá também realizar uma análise que inclui os principais requisitos e fatores do trabalho, através dos modelos TOPSIS e QFD, descritos nas secções 4.5 e 4.4, respetivamente.

4.1 New Concept Development (NCD)

O modelo NCD é um modelo de dividir a parte frontal da inovação em 3 principais partes representadas por uma roda: a parte central, interior e exterior. A central refere-se ao motor que move a roda, como a cultura da empresa e as estratégias de negócio. A parte interior refere-se às cinco fases da elaboração de uma ideia e de um conceito, que irão ser individualmente abordadas posteriormente. A parte exterior refere-se aos fatores externos que ajudam a elaborar a ideia, como a lei, os canais de distribuição, e competição (Dewulf, 2012).

Identificação da Oportunidade
Nesta fase, é identificada qual a oportunidade e o rumo que o projeto pretende prosseguir. As IES da Universidade de Aveiro, Universidade do Porto, e Universidade de Trás-os-Montes e Alto Douro são compostas por equipas de informática e de segurança de informação que têm como valores a constante melhoria dos seus serviços quer à comunidade académica, quer à Administração Pública e aos cidadãos. O desenvolvimento deste projeto resulta não só num

aumento da visibilidade das Universidades, como também promovem o bom desempenho dos seus serviços e credibilidade dos mesmos. Outra oportunidade refere-se à divulgação do serviço e fornecimento do mesmo a empresas interessadas em aumentar a sua qualidade de resposta a incidentes de cibersegurança.

Análise de Oportunidade

De acordo com a Diretiva 2016/1148 do Parlamento Europeu e do Conselho, foram definidas medidas para tornar as redes e os sistemas digitais e essenciais de cada estado-membro seguras para a sua utilização. Esta cultura de cibersegurança é fundamental para a criação de um enquadramento legal para a economia destes países e para o correto funcionamento da sociedade.

Porém, Portugal ainda requer bastante atenção a este tópico, não só relacionado com a celeridade na resposta a incidentes, como também na partilha dos mesmos. As ferramentas atualmente utilizadas não fornecem o suficiente para o estudo e simulação destes ataques, para além de fornecerem formação aos vários profissionais para a sua deteção, mitigação, e partilha dos eventos. Existe, assim, uma carência fundamental de criar novos sistemas para conseguir cumprir estas questões, tanto o tratamento eficiente de resposta a incidentes, como também a aprendizagem a partir dos mesmos de forma rápida eficiente (CNCS - Centro Nacional de Ciber Segurança, 2019).

É de notar também uma grande tendência no aumento do número de incidentes de cibersegurança nos vários setores de áreas governativas, dos quais 9% dos ataques em 2020 foram realizados à Educação e Ciência, Tecnologia e Ensino Superior (ECTES). Aliás, o cibercrime em Portugal tem vindo a aumentar substancialmente em diversos setores (CNCS - Centro Nacional de Cibersegurança, 2021). A título de exemplo, observa-se que foram registados aumentos tanto no número de notificações de burlas informáticas à Polícia Judiciária (mais 22% em 2020 do que em 2019), no número de denúncias recebidas pelo Ministério Público (mais 183% em 2020 do que em 2019) e no aumento do número de ataques classificados como acesso ou interação ilegítima (mais 24% em 2020 do que em 2019), tornando-se, assim, o crime informático mais registado pelas autoridades policiais em 2020 (CNCS - Centro Nacional de Cibersegurança, 2021). É de notar também que a AP é das principais vítimas dos agentes de ameaças, juntamente com as pequenas e médias empresas (PME), os órgãos de soberania, e os cidadãos. Compreende-se, assim, a necessidade crescente de melhor formação na área de cibersegurança e da elaboração de novas soluções e novos modelos de resposta a incidentes e análise de ataques, de maneira a combater de forma eficaz estes números (CNCS - Centro Nacional de Cibersegurança, 2021).

Geração de Ideia

Com base na análise feita, desenvolveu-se a principal abordagem para a solução. Tendo como base experiências passadas em competições CTF nas quais as instituições do Consórcio participaram, foram detetados e analisandos alguns sistemas de Cyber Range, como era o caso da CyberExer e Cyberbit. A ideia pensada foi em utilizar um sistema como estes ou semelhante para atingir o propósito e os objetivos do projeto.

A plataforma que fosse selecionada deveria passar um conjunto de requisitos, como criar um certo número de cenários ou máquinas virtuais para um determinado número de utilizadores. Também se pensou que tipo de artefacto deveria ser feito para comprovar o bom funcionamento da plataforma e como se distribuiria a solução final.

Seleção da Ideia

Tendo por base os requisitos previamente mencionados, foi idealizada a criação de "uma infraestrutura (o CyberLab) capaz de dotar as 3 entidades copromotoras e a administração pública das regiões norte e centro com capacidade para cooperarem e desenvolverem soluções inovadoras e adaptadas ao seu contexto na área da cibersegurança." (Universidade de Aveiro et al., 2019). Este Laboratório de Experimentação terá como principal propósito tanto o estudo e proposta de modelos de segurança adaptados a diferentes ambientes organizacionais, como também a realização de ciberexercícios destinados aos vários profissionais de uma organização, quer ligados à cibersegurança, como também a diversas outras áreas, como marketing, recursos humanos, gestão de topo, entre outros.

Através da aquisição de um serviço *third-party* de laboratório de cibersegurança e de construção de exercícios de segurança informática e Cyber Ranges, pretende-se construir uma solução adaptada ao contexto das IES em questão e sua adaptabilidade aos diferentes âmbitos da AP.

Conceito e desenvolvimento

Depois de identificados os principais requisitos do sistema, procedeu-se à análise do mercado, das soluções existentes, e definição das métricas para o desenvolvimento do projeto. Para além disso, também se aprovou a viabilidade do financiamento do projeto e análise da capacidade das equipas de desenvolvimento de cada IES.

4.2 Modelo CANVAS

O modelo CANVAS é um modelo de estratégia de negócio criado por Alexander Osterwald, em 2005, que tem como objetivo providenciar um modelo visual e intuitivo para qualquer negócio, dividindo-o em ideias chave, como a proposta de valor, os parceiros, e os clientes de qualquer iniciativa ou projeto.

Para este projeto, inicialmente foi adotada uma variação do CANVAS, intitulado Lean CANVAS, mais ajustável às hipóteses iniciais do projeto. As ideias-chave deste modelo assemelham-se as do CANVA e são as seguintes, estando listadas por ordem lógica de preenchimento: problema, segmentos de cliente, proposta de valor único, solução, vantagem, fluxo de receitas, estrutura dos custos, métricas-chave, e canais de relação com o cliente (Skowron, 2020). Porém, como algumas das categorias a preencher não eram necessárias de acordo com as especificidades do projeto (a título de exemplo, definir as métricas imediatamente no início, quais a vantagens cruciais que distinguem da concorrência ou quais os clientes ideias no início do projeto), foi elaborado o modelo CANVAS, que pode ser consultado na figura 1.

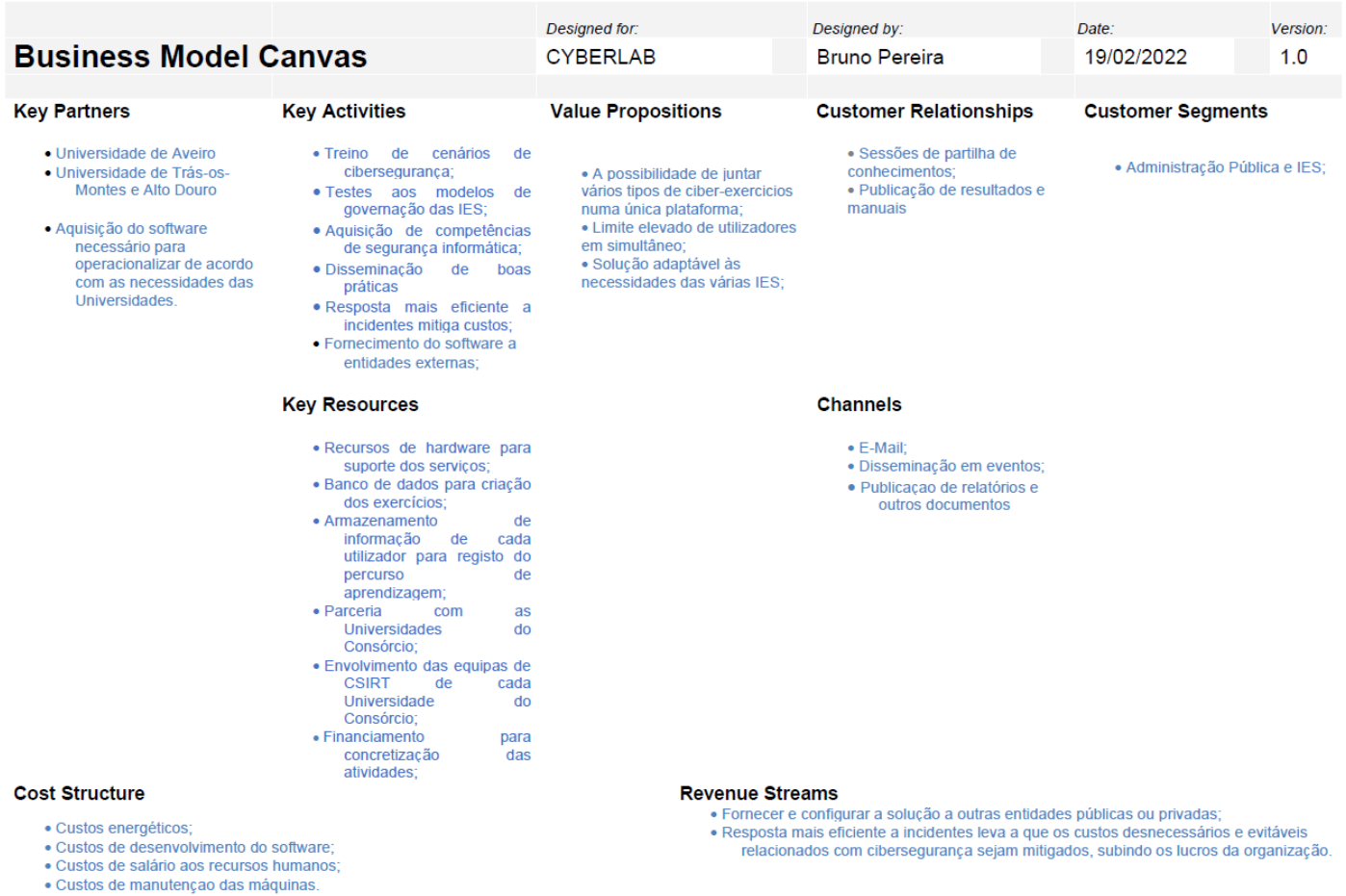

Figura 1 Modelo de negócio CANVAS no âmbito do projeto CyberLab

4.3 Análise SWOT

A análise SWOT (cuja sigla significa forças, fraquezas, oportunidades e ameaças)[2] é uma *framework* usada para identificar os pontos fortes e fracos de um conceito, projeto ou iniciativa, assim como as suas oportunidades e ameaças. Ao analisar os fatores internos e externos de uma organização, esta pode mais facilmente adotar uma melhor decisão para o seu negócio e realizar um balanço do estado da mesma.

Para o projeto CyberLab, a análise SWOT pode ser consultada na tabela 1:

Tabela 1 Análise SWOT

Forças	**Fraquezas**
▪ Capacidade para uma resposta mais eficiente e eficaz na área da cibersegurança; ▪ Normas de referência internacional; ▪ Sessões de sensibilização; ▪ Serviço adaptável ao contexto das IES; ▪ Caráter inovador a nível interno da Administração Pública, contribuindo para a ENSC 2019-2023; ▪ Criação de uma comunidade e parcerias para troca de experiências e partilha sobre os vários ataques ocorridos ou ciberexercícios realizados.	▪ Incapacidade de criar um cenário de cibersegurança com absoluta exatidão ao que acontece na realidade; ▪ Possibilidade de não conseguir cumprir completamente todos os requisitos de certificação internacional;
Oportunidades	**Ameaças**
▪ Disponibilização do serviço a organizações externas; ▪ Apresentação do serviço em Jornadas da Fundação para a Computação Científica Nacional (FCCN);	▪ Elevados custos de energia e manutenção

Através desta tabela, é possível verificar as forças que impulsionam o valor do projeto e, também, verificar quais são os pontos que poderão retirar valor à solução. Desta forma, verifica-se que é necessária mais atenção na aplicação das certificações na solução a desenvolver e na implementação de algoritmos de criação e realização de exercícios. Se se apostar nestas áreas, o CyberLab poderá afirmar-se como uma solução com maior valor para a comunidade e seus clientes.

[2] Traduzido do inglês: Strengths, Weaknesses, Opportunities, Threats

4.4 Análise Quality Function Deployment (QFD)

O modelo QFD foi introduzido pela primeira vez por Yoki Akao (Akao, 1990) com o objetivo de interligar os requisitos do cliente (CR[3]) com os fatores necessários para o desenho do produto ou solução (EC[4]). Através desta interligação, é possível verificar qual a correlação entre os vários EC e os CR, quais o que devem ser tratados com maior importância, e melhorar o planeamento da solução. Este modelo foi aplicado a várias áreas que envolvem gestão e planeamento de linhas de montagem, gestão de projetos, e indústrias (Wu et al., 2020).

Para esta análise, realizou-se a construção de uma House of Quality (HoQ), diagrama onde é possível descrever quais são os CR e EC, qual a correlação entre eles, qual a importância relativa dos CR, como é que os EC se influenciam entre si, e qual a importância de cada EC. É importante realçar que os valores numéricos indicados, assim como a força da relação entre o CR e os EC, correspondem apenas a estimativas que, posteriormente, podem sofrer alterações consoante um input mais preciso por parte dos *stakeholders.* Assim, iniciou-se o processo por identificar quais eram os requisitos do cliente, e o quão importantes são para o mesmo. Estes estão representados na tabela 2.

Tabela 2 Requisitos do Cliente

Requisitos do Cliente	**Peso**
Criar e realizar exercícios e cenários de Cyber Range, CTF, Threat Hunting, etc.	16%
Experimentar e testar modelos operacionais aplicáveis às infraestruturas das Universidades do consórcio	13%
Realizar exercícios conjuntos entre as Universidades e AP.	6%
Acompanhar o percurso de autoaprendizagem do utilizador.	10%
Permitir a evolução contínua dos exercícios	8%
Criação de parcerias de desenvolvimento e investigação	3%
Monitorar e gerir os exercícios em tempo real	10%
Avaliar os exercícios realizados	13%
Permitir a existência de uma UI diferente para cada Team (Red, Blue, White)	16%
Suporte à plataforma realizado a cada 4 anos	3%
Realizar auditorias internas anualmente e rever os processos de negócio bianualmente	3%
TOTAL	**100%**

[3] Do inglês: *client requirements*
[4] Do inglês: *engineering characteristics*

De seguida, definiram-se quais os critérios de engenharia que influenciam estes requisitos. São estes os seguintes:

- Dimensionamento/Quantidade de utilizadores;
- Quantidade de exercícios;
- Quantidade de máquinas e VM em simultâneo;
- Qualidade de automatização da gestão de cenários;
- Recursos (Hardware, concorrência, capacidade de processamento, etc.);
- Diversidade de vulnerabilidades;
- Custos financeiros de implementação;
- Periodicidade de atualizações;
- Duração de sessões de transferência de conhecimento;
- Certificações;
- Modelos de Governação e Processos.

Com isto, definiu-se a relação entre os EC definidos e os requisitos do cliente. O resultado encontra-se na figura 2, juntamente com a legenda das figuras adjacente a essa figura:

Customer Requirements (Explicit and Implicit) \ Functional Requirements	Dimensionamento/Quantidade de utilizadores	Quantidade de exercícios	Quantidade de máquinas e VMs em simultâneo	Qualidade de automatização da gestão de cenários	Recursos (Hardware, concorrência, capacidade de processamento, etc)	Diversidade de vulnerabilidades	Custos financeiros de implementação	Periodicidade de atualizações	Duração de sessões de transferência de conhecimento	Certificações	Modelos de Governação e Processos
Criar e realizar exercícios e cenários de CyberRange, CTF, Threat Hunting, etc	○	●	●	●	●	●		●	○	●	
Experimentar e testar modelos operacionais aplicáveis às infraestruturas das Universidades do consórcio	○		○	●	▽			▽	○	○	●
Realizar exercícios conjuntos entre as Universidades e AP, com partilha de resultados e conhecimentos	●	●	●	●	●	●		●	●	●	
Acompanhar o percurso de auto-aprendizagem do utilizador.		○		●	○	●		○		●	
Permitir a evolução contínua dos exercícios	●	●	●	○	○	▽	▽				
Criação de parcerias de desenvolvimento e investigação			○	●	○	●	●	▽		○	○
Monitorar e gerir os exercícios em tempo real	●	●	●	●	●	○	○	▽			
Avaliar os exercícios realizados			○	●	●	▽			▽		
Permitir a existência de uma UI diferente para cada Team (Red, Blue, White)	▽						▽				
Suporte à plataforma realizado a cada 4 anos						▽	▽	●		○	
Realizar auditorias internas anualmente e rever os processos de negócio bianualmente				○	○	▽	▽	●		○	

Relationships	
Strong	●
Moderate	○
Weak	▽
None	

Figura 2 Relação entre os CR e EC

Posteriormente, definiram-se as correlações entre os EC´s listados, assim como o seu sentido de desenvolvimento. Exemplificando, é desejável que a qualidade de automatismo do laboratório aumente e que os custos de implementação diminuam. Estes valores estão representados por um triângulo preto com o vértice para cima no caso da direção ser positiva, e para baixo no caso de ser negativa. Os valores das correlações estão representados por um símbolo "+" no caso de ser positiva, "- "no caso de ser negativa, e vazio se não existir correlação.

Estas correlações estão representadas na figura 3.

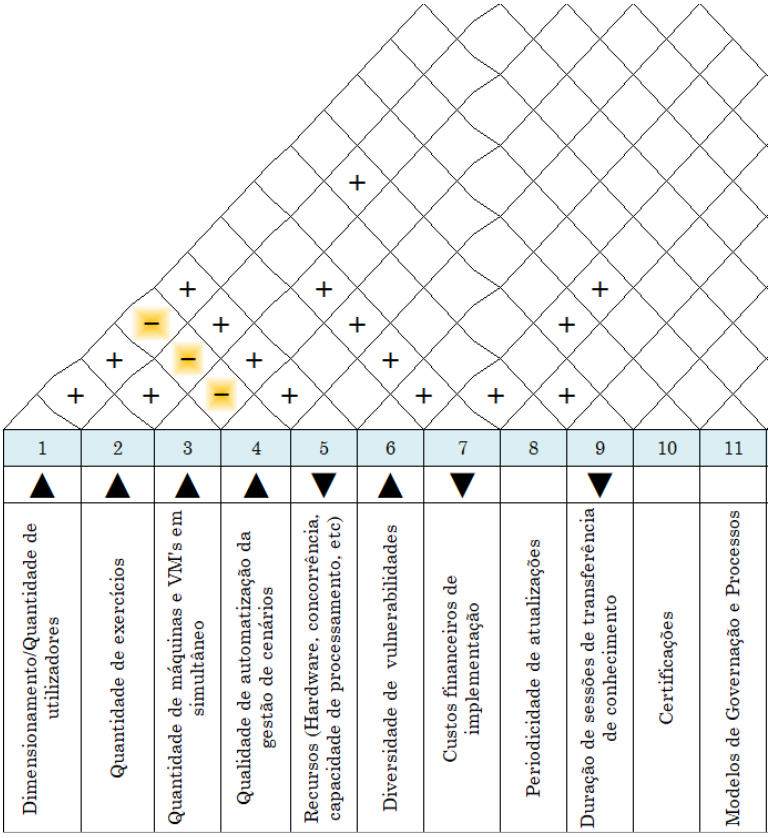

Figura 3 Correlações entre os EC

Executando os cálculos necessários, foram processados os EC para identificar o peso de cada um. Os resultados estão compilados na tabela 3.

Tabela 3 Pesos da Importância dos EC

Requisitos do Cliente	**Rating**	**Peso**
Dimensionamento/Quantidade de utilizadores	315.80	9%
Quantidade de exercícios	385.70	10%
Quantidade de máquinas e VM em simultâneo	442.86	12%
Qualidade de automatização da gestão de cenários;	661.90	18%
Recursos (Hardware, concorrência, capacidade de processamento, etc.)	484.13	13%
Diversidade de vulnerabilidades	369.84	10%
Custos financeiros de implementação	87.30	2%
Periodicidade de atualizações	311.11	8%
Duração de sessões de transferência de conhecimento	155.56	4%
Certificações	352.38	10%
Modelos de Governação e Processo	123.81	3%
TOTAL	**3690.50**	**100%**

É possível verificar que a qualidade de automatização da gestão de cenários é o fator mais importante de desenvolvimento, já que este está presente em vários aspetos, desde a criação dos exercícios, a maneira como são avaliados, como as equipas são monitoradas, e tem influência direta nos recursos de hardware utilizados.

4.5 TOPSIS

TOPSIS é uma técnica utilizada para calcular qual a melhor escolha na tomada de decisão de alternativas, com base nos fatores que influenciam essa escolha (Shih et al., 2007). O TOPSIS consegue isso calculando qual é a escolha que proporciona a distância mais curta da solução ótima e a maior distância da solução menos ótima. As vantagens que este modelo proporciona em relação aos restantes são (Kim et al., 1997):

1. Uma lógica fácil de compreender;
2. Uma forma de considerar a melhor escolha de acordo com a solução ótima e menos ótima;
3. Fórmulas simples capazes de serem computadas numa folha de cálculo.

Os passos para realizar o cálculo da melhor solução usando o TOPSIS são pela seguinte ordem:

1. À semelhança do método AHP, calcular a matriz de comparação par a par de cada fator. A matriz com *i* linhas e *j* colunas deverá ser preenchida segundo a fórmula (1):

$$A = [a_{ij}]$$
$$a_{ij} = \alpha \Rightarrow \; a_{ji} = \frac{1}{\alpha}, \alpha \neq 0, a_{ii} = 1 \tag{1}$$

2. Calcular a matriz normalizada do ponto 1, segundo a fórmula (2):

$$A' = [a'_{ij}] = \frac{a_{ij}}{\sum_{k=1}^{n} a_{ik}}, 1 \leq \mathrm{i} \leq \mathrm{n} \; \wedge \; 1 \leq \mathrm{j} \leq \mathrm{n} \tag{2}$$

3. Calcular o peso de cada fator, que corresponde à média de cada linha;
4. Construir a matriz de decisão, com *n* linhas que representam as alterativas para encontra a solução e *m* colunas que correspondem aos fatores. Nas células dessa matriz devem constar a pontuação de uma alternativa em relação a um critério;
5. Determina-se a matriz normalizada do ponto 4;
6. Multiplicar o peso do ponto 3 para cada critério por cada célula da matriz normalizada do ponto 5;
7. Determinar a solução ideal positiva e negativa para cada critério, que correspondem aos valores máximos e mínimos dessa coluna, respetivamente;
8. Calcular a medida de separação de cada alternativa em relação à solução ótima e não ótima. A separação da solução ótima pode ser calculada com a fórmula (3) (o cálculo da

separação da solução não ótima é semelhante, mas é utilizado o valor mínimo de um critério invés do máximo):

$$S_i^* = \left[\sum_j \left(v_j^* - v_{ij}\right)^2\right]^{\frac{1}{2}}, \mathrm{i} = 1, \ldots, \mathrm{m} \quad (3)$$

9. Calcular a proximidade da solução ideal utilizando a fórmula (4):

$$C_i^* = {S_i'}/{S_i^* + S_i'}, 0 <, C_i^* < 1 \quad (4)$$

Apesar de atualmente não existir informação completamente certa e precisa sobre a classificação das alternativas existentes, já foi construído numa folha de cálculo o modelo e as fórmulas para identificar qual a melhor alternativa, cujos valores das tabelas podem ser consultados no Anexo B. Qualquer valor relatado neste documento corresponde apenas a uma estimativa e pode não corresponder na totalidade à realidade existente da alternativa em questão.

4.5.1 Análise das Alternativas

Tendo em conta os objetivos do projeto, não existe a previsão do desenvolvimento de uma plataforma própria das IES. Desta forma, estará prevista a abertura de um concurso público para que empresas externas possam concorrer de maneira a operacionalizar o software da que for selecionada.

Existem duas empresas cujas soluções são de maior interesse no contexto do projeto. Desta forma, para efeitos de preenchimento do modelo TOPSIS, considerou-se apenas essas duas soluções: a Cyberbit e a CyberExer. Segue-se uma comparação das suas características na tabela 4.

Tabela 4 Comparação das soluções da CyberExer (CyberExer, 2021) e CyberBit (CyberBit, 2022)

CYBEREXER	CYBERBIT
Proporciona ambiente de Cyber Range no âmbito de competições, pesquisa científica, e testagem à resiliência organizacional.	Cyber Ranges focados na simulação de ambientes *cloud* e híbridos
Cyber Ranges customizáveis às necessidades da organização	Uso de ferramentas tais como IBM QRadar, Paloalto Firewall e soluções da McAfee, Windows e Amazon
Cyber Ranges adaptados ao contexto das IES, capazes de simular ambientes próximos da realidade.	Cyber Ranges customizáveis às necessidades da organização
Simulação de redes de infraestruturas críticas	Foco na equipa e na aquisição de competências
Contém biblioteca de alvos pré-feitas	Contém biblioteca de alvos pré-feitas
Serviços de monotorização e pontuação de exercícios de alta qualidade	Contém diversas *dashboards* que analisam várias métricas, desde o impacto da equipa no SOC simulado, como ao progresso dos vários elementos da mesma
Automatização dos cenários através de tecnologia vLab Manager	Fornece diagramas da arquitetura de rede da organização que está a ser atacada.
Soluções tecnológicas *in-house* para auxílio da realização dos cenários e seu planeamento estratégico	Providencia laboratórios para treinar ferramentas de segurança
Fornece serviços de criação de CTF	Cyber Ranges adaptados ao contexto das IES, capazes de simular ambientes próximos da realidade.
Serviços alinhados com os parâmetros da NIST Cybersecurity Framework e na MITRE ATT&CK	Serviços alinhados com os parâmetros da NIST Cybersecurity Framework, NICE Cybersecurity Framework, e na MITRE ATT&CK
Provisiona serviços de treino e formação	Provisiona serviços de treino e formação

Tendo esta informação em consideração, procedeu-se ao preenchimento da folha de cálculo com uma estimativa da pontuação das alternativas face aos fatores. Consideraram-se os seguintes fatores de decisão:

- Quantidade de utilizadores;
- Qualidade dos Exercícios de Cyber Range;
- Qualidade dos Exercícios de CTF;
- Qualidade dos Exercícios de Exercícios de Equipa/Conjuntos;
- Autoaprendizagem;
- Qualidade do Algoritmo de Criação de Exercícios;
- Monotorização;
- Sistema de Pontuação;
- Manutenção (Atualizações, Auditorias, Certificações);
- Testagem de Modelos Operacionais.

A matriz de comparação entre fatores encontra-se representada na figura 4.

Matriz de Comparação										
	Qtd. Utilizadores	Qual. Exer. CyberRange	Qual. Exer. CTF	Qual. Exer. Conjunto	Auto-aprendizagem	Qual. Algoritmo Criação de Exer.	Monotorização	Sistema de Pontuação	Manutenção (Auditorias, atualizações)	Testagem de Modelos Operacionais
Qtd. Utilizadores	1	0.333333333	0.333333333	1	0.5	0.142857143	0.2	0.2	0.333333333	0.5
Qual. Exer. CyberRange	3	1	1	2	3	0.5	2	1	1	1
Qual. Exer. CTF	3	1	1	2	3	0.5	2	1	1	1
Qual. Exer. Conjunto	1	0.5	0.5	1	0.333333333	0.2	0.5	0.5	0.5	1
Auto-aprendizagem	2	0.333333333	0.333333333	3	1	0.142857143	0.333333333	0.333333333	0.5	2
Qual. Algoritmo Criação de Exer.	7	2	2	5	7	1	5	2	1	5
Monotorização	5	0.5	0.5	2	3	0.2	1	1	0.166666667	1
Sistema de Pontuação	5	1	1	2	3	0.5	1	1	0.2	1
Manutenção (Auditorias, atualizações)	3	1	1	2	2	1	6	5	1	0.333333333
Testagem de Modelos Operacionais	2	1	1	1	0.5	0.2	1	1	3	1
SOMA	32	8.666666667	8.666666667	21	23.33333333	4.385714286	19.03333333	13.03333333	8.7	13.83333333

Figura 4 Matriz de Comparação

A classificação de cada alternativa face aos fatores está indicada na tabela 5. É de notar que a pontuação que foi dada tanto na matriz da figura 4 como na tabela 5 partem de uma opinião subjetiva do peso de cada fator e de nada se referem a valores previamente estipulados. Tendo em consideração que esta técnica se baseia em verificar qual a hipótese mais próxima da realidade e tendo que em conta que o peso de cada fator de ambas as empresas podem diferir de acordo com o propósito do projeto, considerou-se aceitável que estes valores sejam subjetivos ao analisador das alternativas.

Tabela 5 Matriz de Decisão

Fatores	**CYBEREXER**	**CYBERBIT**
Quantidade de utilizadores	10	7
Qualidade dos Exercícios de Cyber Range	10	8
Qualidade dos Exercícios de CTF	9	0
Qualidade dos Exercícios de Exercícios de Equipa/Conjuntos	6	9
Autoaprendizagem	8	9
Qualidade do Algoritmo de Criação de Exercícios	9	7
Monotorização	6	8
Sistema de Pontuação	7	7
Manutenção (Atualizações, Auditorias, Certificações)	8	10
Testagem de Modelos Operacionais	0	0

Tendo em consideração a falta de informação relativa à testagem de modelos, não se considerou a pontuação para nenhuma alterativa relativamente a este fator. Com estes valores, a alternativa que mais próxima se encontra da solução ótima é a da CyberExer, com 0.69 valores, comparativamente à da Cyberbit que pontua 0.31 valores.

5 Planeamento dos Ciberexercícios

Neste capítulo encontra-se compilado um guião de como preparar ciberexercício. Esta compilação foi baseada em quatro artigos sobre boas práticas de como realizar este planeamento. Assim, esta parte do documento apresenta quais os benefícios dos ciberexercícios, quais as fases do planeamento, o que deve acontecer quando o exercício decorre e, finalmente, como se deve proceder para a avaliação do mesmo.

5.1 Benefícios

A criação de ciberexercícios numa organização proporciona um ambiente de aprendizagem dentro da mesma, no qual é possível experimentar e testar os procedimentos de segurança e as capacidades dos funcionários dessa instituição ao resolver o exercício proposto. Como a organização necessita de estar preparada para lidar com um incidente de segurança, quer seja na sua deteção ou recuperação, é importante a utilização frequente deste tipo de exercícios, para que as perdas financeiras ou de reputação sejam cada vez menores (Traficom - Finnish Transport and Communications Agency, 2020). Dentro deste ambiente seguro é possível perceber quão resilientes os indivíduos são face aos ciberataques, criando uma cultura de aprendizagem, tanto ativa como passiva, nos vários grupos e indivíduos que realizam o exercício (National Cyber Security Centre, 2020).

5.2 Planeamento

Distribuição da infraestrutura

Existem três formas de classificar um ciberexercício consoante a distribuição do ataque pela(s) organização(ões). Por um lado, muitos ciberexercícios são feitos intra-organizacionalmente, ou seja, uma organização cria o exercício para os seus próprios funcionários. Por outro lado, existem simulações de ataque que podem afetar múltiplas organizações simultaneamente, mas

que não precisam necessariamente de trabalhar entre si para o resolver. Por último, o exercício poderá envolver um ataque que afeta múltiplas empresas parceiras que têm de cooperar entre si para resolver o problema (ENISA - European Union Agency for CyberSecurity, 2009). Note-se que quando se refere a "ataque", pode incluir qualquer efeito indesejável à organização, como por exemplo um desastre natural.

Identificação do Objetivo

Cada ciberexercício deve conter um contexto e um objetivo. Nesse sentido, tem de existir um propósito ou uma análise prévia do estado de arte das vulnerabilidades e da cultura de segurança da empresa para entender qual o procedimento de segurança mais adequado à realidade da empresa. Verbos como "rever", "validar", "desenvolver" ou "explorar" podem ser utilizados para descrever a ação que a empresa pretende executar. Alguns objetivos (Traficom - Finnish Transport and Communications Agency, 2020) podem incluir:

- Recuperar e responder a incidentes;
- Desenvolver capacidades técnicas
- Identificar e detetar de ameaças;
- Testar procedimentos de segurança;
- Realizar documentação e reportes.

A título de exemplo, um bom objetivo seria testar a resposta a incidentes num ataque à base de dados da empresa, ou até explorar o papel da equipa de comunicação aquando de uma disrupção dos serviços centrais de uma universidade (Victoria State Government, 2019).

É importante realizar uma análise de risco na empresa e relacionar o dano potencial de um ataque com a sua probabilidade deste acontecer, de modo a entender os pontos críticos da organização, desenvolver um plano de segurança e testá-lo com o exercício (National Cyber Security Centre, 2020). Recomenda-se neste passo uma reunião com a gestão de topo para auxiliar nesta escolha de objetivo e na concretização do exercício (Victoria State Government, 2019).

Muitas organizações optam por contratar empresas externas para ajudar no planeamento deste ciberexercício. Nesta metodologia, uma empresa pode vir a ter funcionários dedicados a tempo inteiro para trabalhar com os consultores dessa empresa externa para a organização do exercício (ENISA - European Union Agency for CyberSecurity, 2009).

Modelo dos exercícios

Depois de definido o objetivo, é importante selecionar de que forma este exercício irá decorrer.

Uma das principais abordagens é um exercício *tabletop,* que consiste numa sessão de discussão de procedimentos que os participantes terão de ter para entender que ações realizariam naquele determinado contexto. Neste tipo de exercícios, é possível experimentar a tomada de decisões em situações sem a influência de um incidente autêntico. Normalmente estes exercícios são liderados por um facilitador (Victoria State Government, 2019).

Normalmente, este género de exercícios dá maior valor à criação, execução, e revisão de planos de contingência ou de recuperação em caso de desastre. Como existe um maior foco na discussão do contexto, não há uma grande necessidade de criar guiões ou comunicações que vão ocorrendo ao longo do exercício (*injects*). Salienta-se, assim, a capacidade de tomada de decisões por parte dos participantes. Os resultados destas decisões podem ser entregues por escrito (Traficom - Finnish Transport and Communications Agency, 2020).

Existe ainda outra abordagem de fazer ciberexercícios: a *live-play*, nos quais os participantes realizam as suas ações num ambiente simulado e especialmente criado para o contexto do exercício (National Cyber Security Centre, 2020). Este formato permite que a organização teste o seu equipamento e as suas máquinas numa resposta a incidentes.

Neste modelo de exercícios prevalecem os *injects*, que são lançados aos participantes na forma de email, carta, chamada telefónica, entre outros, e que permitem o desenrolar da ação e da história do incidente. O intuito principal desta abordagem é fazer com que os participantes consigam corrigir o problema em questão enquanto têm de lidar com vários eventos ao mesmo tempo, como vários emails, publicações em redes sociais, chamadas telefónicas, entrevistas, etc. Quanto mais preciso for o cenário face à realidade, melhor para os participantes terem uma noção de como têm de agir em determinados contextos. Estes *injects* podem ser controlados e geridos por uma equipa criada especificamente para esse efeito.

A comunicação externa é um aspeto que se considera essencial praticar, pois toda a informação que os media obtêm da equipa desenvolvedora será divulgada nos vários meios de comunicação social e, por isso, é imprescindível ter em atenção aquilo que é transmitido para o público (Traficom - Finnish Transport and Communications Agency, 2020).

A escolha do modelo do exercício deve ter em conta os objetivos que foram traçados, os recursos disponíveis, o tempo de preparação e execução do exercício, e as capacidades dos participantes (National Cyber Security Centre, 2020).

Duração dos exercícios

É difícil prever quanto tempo será necessário para planear o exercício, porque é necessário ter em conta determinados fatores, tais como o tamanho e complexidade do exercício, a sua tipologia, e os recursos disponíveis.

É estimável que um exercício *tabletop* possa ter até 3 meses de preparação, enquanto um grande exercício *live* já demore entre 8 a 18 meses para preparar (ENISA - European Union Agency for CyberSecurity, 2009).

Localização

O espaço onde o exercício possa ser realizado deverá ser grande o suficiente para acomodar os vários equipamentos, materiais e equipas que participarão no exercício. Deverá conter pelo menos as seguintes características (Traficom - Finnish Transport and Communications Agency, 2020):

- Uma sala reservada para os participantes (se houver equipas com tarefas diferentes, será preciso uma sala para cada uma);
- Uma sala para a equipa de controlo do exercício;
- Boa ventilação e/ou ar condicionado;
- Material de escrita;
- Um quadro branco ou um local para afixar documentos ou papéis;
- Comida e bebida se as sessões durarem o dia todo;
- Indicação que existe um exercício a decorrer no edifício.

Equipa de desenvolvimento

De modo a garantir que o exercício é corretamente planeado, monitorizado, e avaliado, é necessária uma equipa dedicada a este efeito. Este planeamento deve ter em consideração que os exercícios são relevantes, realistas, e possíveis de realizar na totalidade. Para além disso, o exercício deverá naturalmente cumprir com os objetivos que foram traçados. Cabe à equipa de desenvolvimento garantir que estes parâmetros são alcançados (National Cyber Security Centre, 2020) (Victoria State Government, 2019).

É recomendável que esta equipa tenha um líder que, neste caso, atuaria como *Project Manager,* e garantiria o bom funcionamento dos restantes elementos. Quando existe uma empresa externa, ou fornecedor de serviços, ou outros parceiros envolvidos na equipa, é boa prática colocar um individuo convidado desse grupo em questão como líder desta equipa. Seguramente, deverá existir membros com elevado conhecimento da estrutura da organização e que se responsabilizem pelo conteúdo do exercício.

Relativamente ao trabalho e tempo investido desta equipa, este deve ser definido e previsto aquando da criação da equipa, já que é preciso todos terem compromisso para comparecer a reuniões e dedicar o seu tempo à criação do exercício. Este trabalho pode depender do modelo do exercício, já que um *tabletop* não tem os mesmos requisitos que um *live-play*. Até pode ser mesmo preferível realizar num ano vários exercícios pequenos em vez de um único exercício complexo (Traficom - Finnish Transport and Communications Agency, 2020).

Calendário de reuniões

A abordagem representada na figura 5 poderá ser utilizada como exemplo para planeamento das reuniões e eventos da equipa de desenvolvimento do exercício.

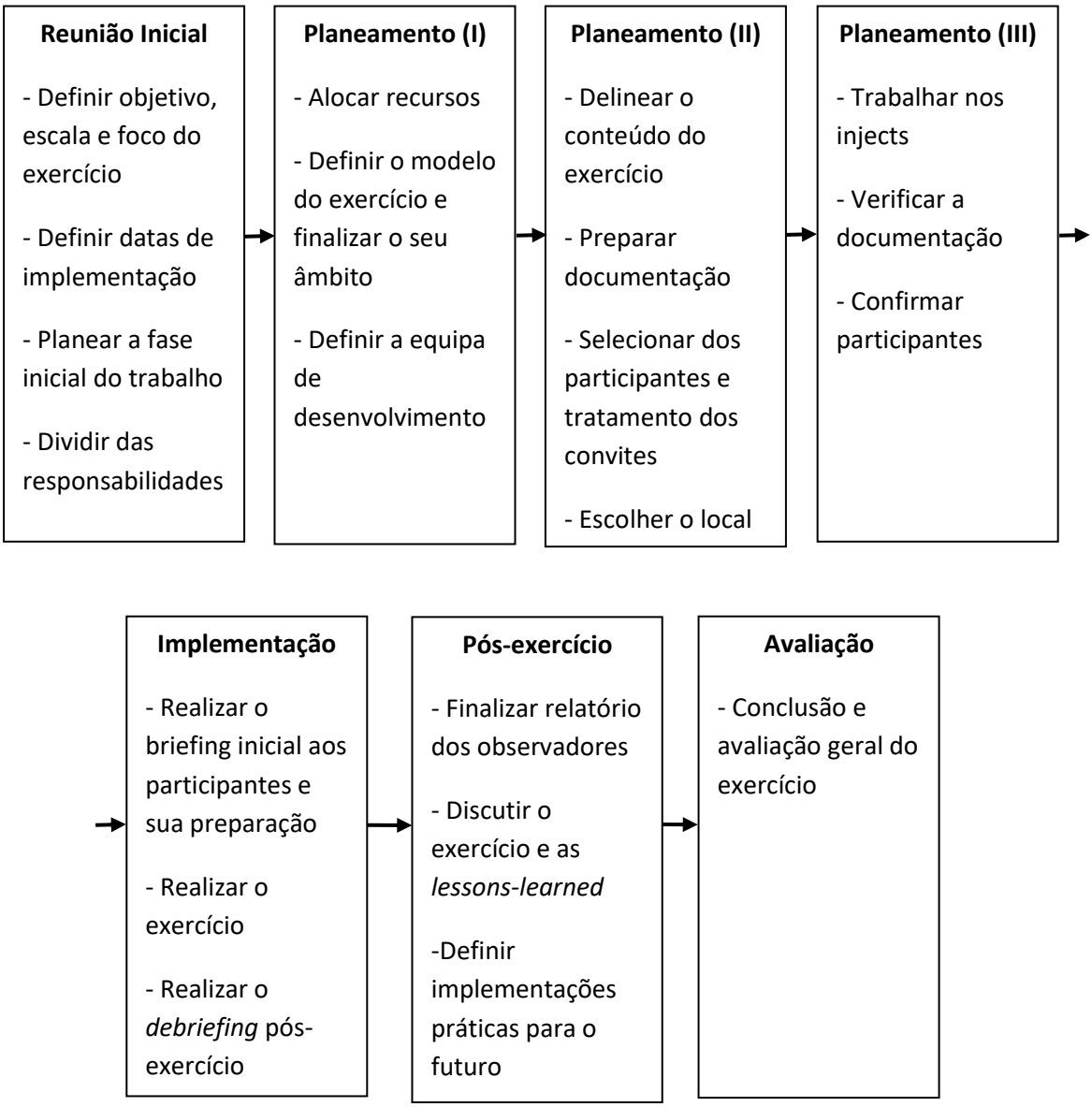

Figura 5 Planeamento das reuniões para o ciberexercício

Desenvolvimento

O primeiro passo, na fase de desenvolvimento, deverá consistir em criar a *storyline* para o exercício. Para escolha do contexto do incidente ou o tipo de ataque, é recomendável procurar informação sobre quais são os ataques mais recentes que têm ocorrido na área em que a organização em questão se insere. Para além disso é importante ter algum conhecimento de como a organização funciona e onde o ataque ou o incidente causaria maior dano, caso seja esse o objetivo do exercício (National Cyber Security Centre, 2020). A título de exemplo, uma

organização pode começar por pensar numa ideia mais generalista do contexto do exercício e, posteriormente, ao longo do tempo, ir acrescentando pormenores e detalhes ao exercício. De modo semelhante, uma empresa pode entrevistar os principais *stakeholders* da organização sobre quais os objetivos a trabalhar e, a partir daí, vão construindo o cenário (ENISA - European Union Agency for CyberSecurity, 2009).

Durante a criação deste cenário, também é necessário ter em conta o papel dos moderadores, já que devem ser flexíveis nas interações com a(s) equipa(s) participante(s), tanto a nível das respostas e mensagens que lhes são dadas, como à intimidação que lhe(s) coloca(m). É também importante pensar na forma que estas comunicações, quer internas quer externas, irão decorrer ao longo do exercício (National Cyber Security Centre, 2020).

Do mesmo modo, é importante que os cenários consigam dar flexibilidade aos participantes, dando-lhes possibilidade de realizar várias ações no exercício. Os participantes acabam também por ser imprevisíveis e, por muito que um cenário esteja bem preparado, é provável que irá acontecer sempre alguma dúvida ou ação por parte dos participantes que a equipa de desenvolvimento não esteja a contar (ENISA - European Union Agency for CyberSecurity, 2009).

Relativamente aos *injects,* é crucial que estes sejam claros e bem escritos, de modo a não causar confusão por parte dos participantes. Estes *injects* devem passar por alguém com experiência, para garantir que o que está escrito é correto e não causaria qualquer interrupção indesejada no decorrer do exercício. Para além disso, é relevante que estes *injects* estejam marcados com uma indicação de que são exercícios. Por exemplo, se o *inject* for um email, colocar no "Assunto" do email algo como "EXERCICIO – EXERCICIO – EXERCICIO" (ENISA - European Union Agency for CyberSecurity, 2009, National Cyber Security Centre, 2020).

De seguida, é essencial definir-se como irá ser feita a avaliação do ciberexercício. Para tal, é necessário identificar quais as métricas que se pretende medir e entender o que correu melhor e o que correu pior no exercício. Desta forma, é facilitada a tarefa de identificar as conclusões e as *lessons-learned* do exercício. Alguns exemplos de métricas podem ser:

- Aderência dos participantes ao plano de segurança previsto para o exercício em questão;
- Qualidade das decisões tomadas;
- Qualidade do material produzido;
- Tempo usado a realizar as tarefas.

Finalmente, é importante preparar os guiões para os participantes, para que possam, com alguns dias de antecedência, inteirar-se com as regras, preparar-se para o evento, e entender o que deles é esperado (National Cyber Security Centre, 2020).

Documentação

Os documentos a serem produzidos dependem do que será relevante produzir de acordo com a equipa de planeamento. Alguns exemplos são (Victoria State Government, 2019):

- Conceito: contem os objetivos e conteúdo principal do exercício, assim como dados relativos à logística, financiamento e participantes do mesmo;
- Caderno de Participante: contem regras e instruções para os participantes, assim como o objetivo do exercício, horário, e informação suplementar;
- Caderno do Monitor: semelhante ao Caderno do Participante, no qual se inclui o cenário e os problemas que os participantes pretendem resolver, assim como as alturas previstas de inserir os *injects* no fluxo do exercício;
- Caderno de Controlo: este é opcional e é semelhante ao Caderno do Monitor. Pode conter mais informação detalhada de como avaliar o exercício ou quais as resoluções previstas dos cenários.

Participantes

Até agora, as secções deste capítulo focaram-se nas componentes não-humanas do exercício (com exceção da composição da equipa de desenvolvimento), como o local, a duração do exercício, os cenários e os *injects*, e o modelo de exercício. Contudo, agora é fundamental planear que indivíduos e equipas se irão envolver no ciberexercício.

A escolha dos participantes depende do objetivo do exercício. Se o objetivo for algo como "testar um procedimento dentro da minha organização", então é recomendável que os participantes sejam membros da própria organização. Por outro lado, se o objetivo for algo como "realizar um torneio a nível nacional para averiguar o estado de maturidade dos serviços públicos", então os participantes já serão alguns membros de vários organismos públicos que serão convidados a participar no exercício. Cabe à equipa planeadora definir qual o critério que considere mais relevante nesta escolha

Sem uma equipa participante, o exercício não pode decorrer. Sendo uma parte tão essencial deste processo, deverá ser pensada com cuidado. Isto porque as pessoas baseiam as suas ações na sua motivação para as realizar e, sem a adequada motivação, poderá existir desinteresse em participar no evento. As razões desta desmotivação podem ser várias. As organizações podem estar desconfiadas quanto às regras da confidencialidade, podem não entender os benefícios do exercício, ou podem não ter recursos humanos suficientes para ingressar nestes eventos.

Uma boa forma de cativar estes participantes é através da sensibilização para os benefícios do exercício. Se for possível levantar questões como: "será que a vossa equipa está efetivamente preparada para lidar com incidentes de segurança?"; "será que têm as ferramentas de identificação e deteção de incidentes adequadas?"; "não seria benéfico construir uma parecia mais forte com uma outra organização?"; e "os vossos clientes, parceiros e autoridades não confiariam mais na vossa organização se tivessem a certeza que estão cientes dos ciber-ataques mais atuais e como se defender deles?". A partir do momento que uma equipa participa num exercício que foca nestes pontos, terá interesse em participar em mais ou comunicar a sua experiência com outras equipas.

Outra forma de motivar os possíveis participantes é através de pequenos eventos, *webinars,* ou workshops sobre vulnerabilidades e como nos protegermos delas. Isto envolve todos os

stakeholders numa discussão, na qual pode haver partilha de ideias e, como tal, gerar interesse para o tema.

Um fator que também é importante é a noção de "confiança". Nos últimos anos, organizações destacaram a confiança que desenvolvem ao longo do tempo, quer intra-organização, quer inter-organização, como um grande fator de motivação de participação nos exercícios. Desta forma, recomenda-se que os primeiros exercícios para os participantes que nunca participaram num ciberexercício tenham propósitos mais simples e mais baseados em comunicação entre equipas do que numa vulnerabilidade propriamente dita, de forma a lentamente construir esta confiança entre os participantes.

Em último caso, o financiamento de determinadas partes do exercício pode ser usado como fator motivacional, tal como cobrir custos de alojamento, deslocação, alimentação, ou mesmo através de prémios. Porém, nem todas as equipas terão obrigatoriamente grandes fundos para o planeamento dos exercícios, pelo que é um fator que terá de ser ajustado à equipa desenvolvedora em questão (ENISA - European Union Agency for CyberSecurity, 2009).

Monitores

Os monitores são membros da equipa organizadoras que zelam pelo bom, correto, e eficiente decorrer do exercício. As suas tarefas incluem ações tais como:

- Observar os participantes e as suas ações, assim como reportar informação aos moderadores/equipa de desenvolvimento;
- Direcionar os *injects* aos participantes;
- Responder a questões.

O facto de ter monitores pode causar algum desconforto e pressão nos participantes e, por isso, devem tentar ser imparciais e ubíquos com o ambiente do exercício. O seu papel é importante para garantir uma boa coleção de resultados e feedback dos participantes, de modo a usar essa informação no momento de avaliação e *lessons-learned* (ENISA - European Union Agency for CyberSecurity, 2009).

Observadores

A inclusão de observadores no exercício é opcional e a equipa organizadora deve considerar o seu envolvimento no mesmo. Normalmente, observadores são empresas externas, mas relevantes para o exercício, tais como autoridades públicas, gestores de infraestruturas críticas de outros locais, etc. (ENISA - European Union Agency for CyberSecurity, 2009).

Observar o exercício também pode ser uma boa forma de entender o seu funcionamento, caso os participantes não tenham muita experiência neste tipo de eventos. Alguns envolvimentos podem ser, tal como os monitores, relatar o progresso dos participantes, ou produzir um memorando com as suas observações. Vários observadores podem olhar para diferentes áreas de um exercício. Assim, os apontamentos que os observadores escrevem podem ser partilhados com os participantes e com a equipa organizadora, não só para ajudar no momento de avaliação,

mas também para relatar aos participantes as suas ações, de modo a serem melhoradas no futuro.

Outro observador interessante pode ser os media, de modo a simular o que diriam os participantes ao público em massa no evento do ciberataque em questão. Contudo, isto tem implicações, tais como ser necessário discutir a política e os termos que os media terão de seguir durante o exercício. De qualquer forma, se o exercício for de uma magnitude mais elevada, poderá ser necessário informar os media, de maneira a não confundirem o exercício com um ciberataque verdadeiro.

5.3 Decorrer do Exercício

Informações Iniciais

Nos primeiros momentos do evento, será necessária uma apresentação inicial das regaras e procedimentos aos participantes acerca do exercício. Poderá até mesmo existir um *webinar* antes do dia em que o exercício começa. Nestes momentos, devem ser indicadas as ferramentas que terão de usar, o horário, a lista de participantes, e uma apresentação sobre o contexto do exercício ou tópicos sobre a vulnerabilidade que irá ser explorada (ENISA - European Union Agency for CyberSecurity, 2009).

Desenrolar do Exercício e sua Monitorização

Por esta altura, as instruções e o enunciado do exercício já será dado aos participantes, após estes se deslocarem aos seus locais designados para a realização do exercício. Enquanto os participantes estarão a tomar as suas decisões e a realizar as suas ações, haverá monitores no terreno a observá-los, assim como tomar notas do que fazem e da sua eficiência em resolver o desafio.

Os monitores relatarão as suas conclusões dos participantes à equipa desenvolvedora ao longo do tempo para que consigam acompanhar o desenvolvimento do progresso dos participantes e determinar os próximos passos, incluindo instruir aos monitores para comunicarem o próximo *inject*. A equipa desenvolvedora pode gerir estes *injects* através de um software especializado, ou através de um guião. De modo a facilitar esta tarefa, recomenda-se o uso de uma ferramenta de comunicação (ENISA - European Union Agency for CyberSecurity, 2009).

Estes *injects* podem ser enviados para equipas diferentes em simultâneo se estiverem a desempenhar funções diferentes. Alguns exemplos de *injects* podem ser emails, chamadas telefónicas, entrevistas, notificações às autoridades, ou pedidos urgentes (Traficom - Finnish Transport and Communications Agency, 2020).

5.4 Avaliação

A ideia principal da fase de avaliação é perceber as *lessons-learned*, os problemas que surgiram e os procedimentos que foram executados e os que poderiam ter sido feitos para que o exercício fosse realizado com sucesso, caso esse não seja o caso.

É recomendável que o processo de avaliação seja planeado com antecedência, assim como os seus objetivos e procedimentos de colecionar a informação. Os objetivos devem seguir a regra SMART, isto é, específicos (Specific), mensuráveis (Measurable), atingíveis (Attainable), relevantes (Relevant), e com tempo limite (Time-Bound).

Quanto ao prazo de publicação dos resultados da avaliação, é aconselhável que seja o mais breve possível. Não só porque as *lessons-learned* serão mais fáceis de absorver por parte dos participantes, mas também porque os seus níveis de interesse e motivação para aprender são mais elevados nesta fase.

É necessário ter algum cuidado com o processo de avaliação, já que pode conter informação sensível sobre detalhes da empresa ou possíveis vulnerabilidades. Para além disso, é aconselhável que os relatórios finais não culpabilizem ou humilhem os participantes (ENISA - European Union Agency for CyberSecurity, 2009).

Relatórios
Existem vários tipos de relatórios que podem ser produzidos durante a fase de avaliação:

- **Individual:** Um relatório focado em cada *stakeholder*, com os detalhes das suas ações e conselhos
- **Grupo:** Um relatório focado nos problemas e ações gerais e áreas que necessitam de melhorias. É importante que este relatório não identifique quem realizou cada passo.
- **Público:** É a versão final que apenas inclui informação geral sobre o exercício, sem identificar atores, organizações e vulnerabilidades. Este poderá ser partilhado com os media e o público.

Medir o Sucesso
De modo a verificar se o exercício cumpriu os objetivos que se propôs, a equipa organizadora pode "medir" este sucesso através da forma que achar mais conveniente. Alguns exemplos são:

- **Questionários:** Através de uma pré e pós análise do exercício, de modo a verificar se a visão dos participantes nas temáticas abordadas mudou e entender as *lessons-learned;*
- **Testes de Repetição:** Realizar a mesma tarefa ao longo do exercício, de modo a perceber a evolução da eficácia dos participantes ao realizá-la;
- **Seguimento Pós-Exercício:** Acompanhar os participantes ao longo do tempo após o exercício e verificar que aplicam as correções aos problemas que encontraram durante o exercício.

Em contrapartida, os benefícios do exercício são mais difíceis de medir. Por exemplo, é difícil avaliar como melhorar a cooperação entre as instituições que participaram no exercício ou até mesmo o quão sensibilizados estão perante o problema encontrado (ENISA - European Union Agency for CyberSecurity, 2009).

Feedback

Após o exercício, deverá ser enviada uma mensagem de agradecimento aos participantes, assim como um formulário de avaliação do exercício. Para além disso, é aconselhável transmitir uma mensagem geral aos participantes, informando das conclusões do exercício (Traficom - Finnish Transport and Communications Agency, 2020).

5.5 Análise das Práticas Indicadas

Embora toda a informação que aqui foi exposta seja relativa a quatro guiões de ciberexercícios de agências de nacionalidades diferentes, todos mostraram possuir bastantes aspetos em comum, sendo que, ocasionalmente, a informação contida num guião complementava a de outro guião. Como Portugal se encontra na União Europeia, deu-se uma maior ênfase no artigo da ENISA. Para além disso, era o artigo mais longo e completo dos quatro.

Os guiões comprovaram ser bastante plenos na sua informação, já que abordavam, de forma mais ou menos detalhada, todos as temáticas e passos para planear, executar, e avaliar um ciberexercício. Contudo, a presença de exemplos de exercícios era escassa, sendo que apenas o artigo da ENISA fornecia informações para alguns ciberexercícios que foram realizados no passado. Apesar de, falando na generalidade, os passos para planear estes exercícios abordarem várias possibilidades distintas (por exemplo, explica na íntegra, qual a diferença entre um exercício *tabletop* e *live-play*), muitas vezes não foram apresentados exemplos de como realizar estes passos ou, melhor ainda, não foram apresentados esquemas suficientes ou exemplos de exercícios completos disponíveis para a comunidade em geral.

Dando um maior foco nos aspetos positivos, os guiões mostraram ser eficazes em explicar este planeamento. Caso um organizador nunca tenha tido a experiência de planear um exercício do início ao fim e caso este seja o seu primeiro planeamento, poderá deparar-se com perguntas tais como “Qual o primeiro passo?”, ou “Qual é a lista de tarefas que é suposto estar feita quando o evento começar?”. A compilação de informação neste capítulo ajudará o leitor a responder a tais questões e a construir um exercício com sucesso.

6 Exercícios Desenvolvidos

O capítulo anterior deu a conhecer algumas guias de como fazer um ciberexercício. O presente capítulo já terá como objetivo aplicar os conhecimentos adquiridos no capítulo anterior e construir dois exercícios que servirão como exemplo. Ambos os exercícios terão como tema o serem realizados num ambiente de uma IES. O primeiro exercício consiste num *tabletop,* mais simples, e o segundo exercício consiste numa *live-play* entre a equipa vermelha (atacante) e equipa azul (defesa).

Os exercícios irão usar o capítulo anterior como guia e terão uma lista de tarefas, as quais incluem um responsável, uma data-limite exemplo, e a resolução dessa tarefa. Esta lista poderá ser consultada em formato de tabela no Anexo C.

6.1 Exercício 1 – Tabletop Ransomware (Lockbit)

6.1.1 Identificação do Exercício

Identificar objetivo do exercício
Responsável: Organizador
Data-Limite: 28/09
Descrição: Testar a capacidade de decisão da equipa de segurança da Universidade do Porto e Universidade de Trás-os-Montes e Alto Douro aquando é atacada por um Lockbit Ransomware

Identificar participantes
Responsável: Organizador
Data-Limite: 28/09
Descrição:

- Membros integrantes da equipa de segurança das universidades envolvidas
- Membros integrantes da equipa de proteção de dados das universidades envolvidas

Identificar tipo de exercício
Responsável: Organizador
Data-Limite: 28/09
Descrição: Exercício Tabletop

Identificar *stakeholders*
Responsável: Organizador
Data-Limite: 28/09
Descrição:

- Gestão de topo
- Direções das Faculdades
- Estudantes
- Serviços Administrativos
- Serviços IT

6.1.2 Planeamento

Realizar esquema e objetivos de futuras reuniões
Responsável: Organizador e equipa planeadora
Data-Limite: 29/09
Descrição: Equipa organizadora será composta por 3 membros da unidade de segurança de informação, 3 membros da equipa de redes e 2 membros da unidade de proteção de dados da Universidade de Aveiro.
Esta equipa será dividida em 3 e a sua distribuição de tarefas encontra-se representada na tabela 6.

Tabela 6 Esquema de Reuniões do Exercício 1

	Equipa 1	**Equipa 2**	**Equipa 3**
Reunião 1	- Definir Datas - Definir as metodologias de avaliação	- Preparar *inject* 1 - Definir observadores	- Preparar *inject* 2 - Definir monitores e moderadores
Reunião 2	- Treinar moderadores e monitores	- Preparar o Manual do Participante	- Convidar participantes - Preparar Manual dos Monitores - Preparar Questionário de Feedback
Reunião 3	Reunião extra para delinear preparativos finais		

Definir data e local do exercício
Responsável: Organizador e equipa planeadora
Data-Limite: 29/09
Descrição:

Data: 13/10
Local: Instalações de uma das IES

Preparar *injects* e enunciados do exercício
Responsável: Equipa planeadora
Data-Limite: 03/10
Descrição:

No contexto da rede EWP, rede que interliga digitalmente os serviços de mobilidade de estudantes entre as várias universidades dos Estados-Membros da Europa, foi realizado um acordo com um fornecedor de serviços de mobilidades de estudantes da Arménia, chamada ArmiStudents, para que estudantes desta nação pudessem ter a oportunidade de estudar num país da União Europeia.

Tendo em conta a tensão política e os conflitos do Alto Carabaque, a acontecerem entre Arménia e Azerbaijão, este último ameaça retaliação face a este acordo.

Algumas semanas depois, no dia 13 de outubro, U.Porto e UTAD receberam alertas no seu email de incidentes, informando que as equipas de sistemas de informação não estão a conseguir aceder ao Portal de gestão da Universidade. Apenas aparecem páginas em branco quando tentam iniciar sessão.

Inject 1:

Após alguma análise, descobre-se que um membro da equipa de design gráfico das duas universidades recebeu um email há 5 dias sobre de um concurso de fotografia a decorrer na universidade. Nesse email, estava indicado que, caso o leitor quisesse mais informações, para clicar numa hiperligação, que os redirecionava para uma página na internet em branco.

Para além disso, uma das bases de dados que continha informação sobre o percurso académico dos estudantes foi bloqueada, sendo que foi adicionada uma tabela que contem uma linha a dizer para pagar em criptomoedas aos atacantes de modo a recuperar os seus dados, sob pena de os libertar no mercado negro.

Inject 2:

Mais tarde nesse dia, a equipa recebeu uma chamada de uma universidade francesa, reportando um problema semelhante. Aparentemente, o *malware* que corrompeu os serviços das universidades portuguesas, auto-replicou-se e começou a afetar universidade de outros países europeus.

Para além disso, a equipa de redes descobriu que as configurações de *firewall* das universidades encontravam-se desativadas. (enviado apenas para a equipa de segurança).

Definir monitores e observadores
Responsável: Organizador e equipa planeadora
Data-Limite: 03/10
Descrição:

Monitores:

- Coordenador de segurança de informação da Universidade do Porto
- Coordenador de redes da Universidade do Porto
- Coordenador de segurança de informação da Universidade de Trás-os-Montes e Alto Douro
- Coordenador de redes da Universidade de Trás-os-Montes e Alto Douro

Observadores:

- Gestão de Topo
- Equipa de comunicação das universidades envolvidas
- Membros do jurídico das universidades envolvidas

Definir metodologias de avaliação
Responsável: Equipa planeadora
Data-Limite: 03/10
Descrição:

- A equipa definiu corretamente os processos e procedimentos a executar para recuperar do ataque através da entrega de um relatório de ponto de situação.
- A equipa coordenou e distribuiu tarefas
- A equipa definiu prioridades nas tarefas do plano de reposta a incidentes
- A equipa identificou que serviço interno das universidades deveria contactar
- A equipa identificou que serviço externo das universidades deveria contactar
- A equipa identificou medidas de mitigação do exercício (passwords fortes, *multifactor authentication,* "limpar" contas antigas de docentes, não docentes, estudantes e investigadores, verificação dos backups de dados)

Preparar Caderno de Participante e de Monitor
Responsável: Equipa planeadora
Data-Limite: 13/10
Descrição:

Tendo em conta a duração do exercício, este terá um formato mais simples.
O Caderno deverá conter as seguintes partes:

- Objetivo do exercício
- Objetivos de aprendizagem
- Horário dos acontecimentos (Briefing dos participantes, começo e fim do exercício, sessão de feedback)
- Introdução do cenário
- Critérios de avaliação

O Caderno de Monitor irá conter, adicionalmente aos pontos acima indicados, os *injects* e as fases do exercício.

Preparar questionário de avaliação
Responsável: Equipa planeadora
Data-Limite: 13/10
Descrição:

O questionário terá como objetivo dar voz aos participantes e pedir opinião sobre as temáticas do exercício. Podem conter perguntas sobre:

- Como avaliam o exercício e os *injects*?
- Foi útil para perceber as falhas que têm nas suas organizações?
- Foi acessível em termos de dificuldade e tempo?
- O espaço é adequado?

Treinar monitores e moderadores
Responsável: Equipa planeadora
Data-Limite: 10/10
Descrição: A sessão terá de abordar temáticas, tais como: o que é um Lockbit Ransomware, como funciona, e como mitigá-lo; qual o estado de maturidade de resposta a incidentes das universidades envolvidas; como mandarão os *injects* e quais os canais de comunicação; e o horário do dia do exercício.

Convidar participantes, observadores e media
Responsável: Equipa planeadora
Data-Limite: 04/10
Descrição: O convite pode ser de acordo com as preferências dos organizadores.

6.1.3 Decorrer do Exercício

Sessão inicial dos participantes
Responsável: Equipa planeadora
Data-Limite: 13/10
Descrição:

- Entrega de brindes e do caderno de participante.
- Explicação das regras do desafio.

Executar o cenário e os *injects*
Responsável: Monitores
Data-Limite: 13/10
Descrição:

- O texto introdutório será fornecido no início do cenário.
- O inject 1 será introduzido 20 minutos depois do tempo de início.
- O Inject 2 será introduzido 1 hora depois do tempo de início.

Observar participantes e tirar notas, comparando com o cenário expectável e *checklists*
Responsável: Monitores
Data-Limite: 13/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.3, secção "Desenrolar do Exercício e sua Monitorização".

Relatar decisões dos participantes à equipa organizadora
Responsável: Monitores
Data-Limite: 13/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.3, secção "Desenrolar do Exercício e sua Monitorização".

6.1.4 Avaliação

Responder a questionários
Responsável: Participantes e Monitores
Data-Limite: 14/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Medir o Sucesso".

Compilar e avaliar resultados dos questionários e *feedback* dos monitores
Responsável: Equipa avaliadora
Data-Limite: 13/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Medir o Sucesso".

Preparar o relatório individual
Responsável: Equipa avaliadora
Data-Limite: 15/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Relatórios".

Preparar o relatório de grupo
Responsável: Equipa avaliadora
Data-Limite: 15/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Relatórios".

Preparar o relatório público
Responsável: Equipa avaliadora
Data-Limite: 15/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Relatórios".

Apresentar principais conclusões com os *stakeholders*
Responsável: Equipa avaliadora
Data-Limite: 16/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Medir o Sucesso".

Reunião futura de ponto de situação com os *stakeholders*
Responsável: Equipa avaliadora
Data-Limite: 21/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Medir o Sucesso".

6.2 Exercício 2 – Red Team vs Blue Team

6.2.1 Identificação do Exercício

Identificar objetivo do exercício
Responsável: Organizador
Data-Limite: 28/09
Descrição:

- Testar as capacidades dos participantes quanto às seguintes áreas:
    - Deteção e prevenção de ciberataques
    - Monitorização de rede
    - Controlo da atividade nos sistemas da organização
    - Trabalho em Equipa
- Dividir os participantes em equipa vermelha e equipa azul. Uma para atacar e outra para defender.

Identificar participantes
Responsável: Organizador
Data-Limite: 28/09
Descrição:

- IT e Redes
- Segurança de Informação
- Helpdesk
- Proteção de dados
- Equipa do Jurídico

Os participantes serão divididos em duas equipas: a vermelha (RT) e a azul (BT). A primeira tem como objetivo realizar atividades ofensivas contra a infraestrutura da última. É expectável que a equipa vermelha realize atividades como ataques contra as *workstations* dos utilizadores, instalar *backdoors*, apagar os logs da sua atividade, exfiltrar informação, etc. Por outro lado, é expectável que a equipa azul consiga procurar vulnerabilidades na sua rede, configurar *firewalls*, configurar o seu Intrusion Detection System (IDS), recupere os sistemas comprometidos e reporte os resultados.

Identificar tipo de exercício
Responsável: Organizador
Data-Limite: 28/09
Descrição: Exercício Live Play numa plataforma de CyberRange

Identificar *stakeholders*
Responsável: Organizador
Data-Limite: 28/09
Descrição:

- Gestão de topo
- Direções das Faculdades
- Estudantes
- Serviços Administrativos
- Serviços IT

6.2.2 Planeamento

Realizar esquema e objetivos de futuras reuniões
Responsável: Organizador e equipa planeadora
Data-Limite: 29/09
Descrição:

Equipa organizadora consistirá numa empresa externa.

Esta equipa será dividida em 3 e a sua distribuição de tarefas encontra-se representada na tabela 7.

Tabela 7 Esquema de Reuniões do Exercício 2

	Equipa 1	**Equipa 2**	**Equipa 3**
Reunião 1	- Definir Datas - Definir as metodologias de avaliação	- Preparar *injects* - Definir observadores	- Preparar *injects* - Definir monitores e moderadores
Reunião 2	- Preparar política dos media - Treinar moderadores e monitores	- Preparar o Manual do Participante	- Convidar participantes - Preparar Manual dos Monitores - Preparar Questionário de Feedback
Reunião 3	Reunião extra para delinear preparativos finais		

Definir data e local do exercício
Responsável: Organizador e equipa planeadora
Data-Limite: 29/09
Descrição:

Data: 13/10 – 15/10
Local: Alfândega do Porto

Preparar *injects* e enunciados do exercício
Responsável: Equipa planeadora
Data-Limite: 03/10
Descrição:

A Universidade do Douro Litoral foi recentemente fundada e os seus serviços informáticos têm sido lentamente implementados por uma pequena equipa de engenheiros de software. Tendo em conta o número crescente de ciberataques às instituições de ensino superior, e tendo em conta que muitos dos serviços da universidade já se encontram em produção e com dados dos estudantes, a probabilidade e o impacto de um ataque ocorrerem são elevados.
Tendo isto em conta, a Direção de Ensino Superior do Norte destacou-te como parte do grupo responsável por defender esta infraestrutura. Como tal, tens a missão de detetar e prevenir futuros ciberataques, fornecer relatórios do ponto de situação do sistema, e resolver problemas nas máquinas da universidade em caso de ataque. A arquitetura deste exercício está representada na figura 6.

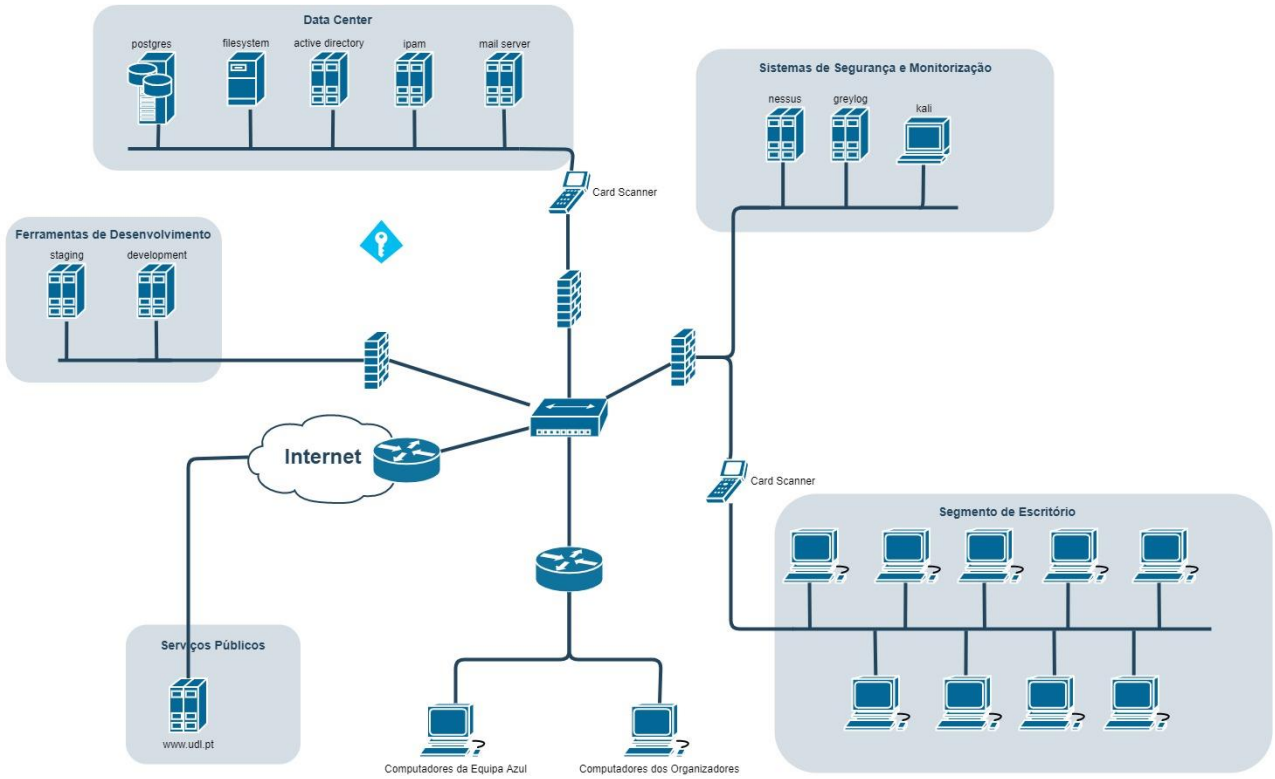

Figura 6 Arquitetura do Sistema do Exercício 2

Inject 1: Ar condicionado
Requisito: Conseguir clonar cartões
Descrição: A equipa azul receberá um email, informando que o sistema de refrigeração do Data Center foi desativado. Isso só é possível porque alguém deve ter acedido ao interior das

instalações e manualmente ter desativado os ares condicionados. Neste momento, todos os *servers* do Data Center encontram-se desativados por sobreaquecimento.

Inject 2: Clonagem do website
Requisito: Ter acesso aos serviços públicos
Descrição: A equipa azul receberá um telefonema de um estudante, informando que, quando tentou aceder ao website da universidade, tentou fazer login na sua conta. Apesar de ter colocado a password correta, o website disse que a password estava errada. Porém, na segunda tentativa de login, já funcionou. O estudante quer verificar se está tudo bem ou se algum incidente ocorreu.

Definir agenda do evento
Responsável: Organizador e equipa planeadora
Data-Limite: 08/10
Descrição:

Dia 1:

- 09:00 – 09:30 – Check-in
- 09:30 – 11:00 – Briefing das equipas e Familiarização do ambiente do exercício
- 11:00 – 11:15 – Coffee Break
- 11h15 – 12:00 – Verificação dos canais de comunicação
- 12:00 – 13:00 – Almoço
- 13:00 – 14:30 – Reunião interna das equipas para definir estratégias
- 14:30 – 14:45 – Coffee Break
- 14:45 – 15:15 – Continuação das reuniões internas
- 15:15 – 15:45 – Sessão de Feedback do dia
- 15:45 – 16.00 – Revert das configurações iniciais dos sistemas.

Dia 2:

- 09:00 – 09:10 – Sessão de abertura
- 09:10 – 09:15 – Briefing inicial
- 09:15 – 12:00 – STARTEX (início do exercício)
- 12:00 – Prazo de Entrega para Situation Report I (SITREP I)
- 12:00 – 13:30 – Almoço (exercício continua)
- 15:30 – Prazo de Entrega para Situation Report II (SITREP II)
- 16:30 – Fim do dia 2
- 16:40 – 17:00 – Sessão de Feedback

Dia 3

- 09:00 – 09:10 – Sessão de abertura
- 09:10 – 09:15 – Briefing inicial do dia
- 12:00 – Prazo de Entrega para Situation Report III (SITREP III)
- 12:00 – 13:30 – Almoço (exercício continua)
- 15:30 – Prazo de Entrega para Situation Report IV (SITREP IV)
- 15:30 – ENDEX (fim do exercício)
- 15:45 – 16:00 – Sessão final

Definir canais de comunicação
Responsável: Organizador e equipa planeadora
Data-Limite: 04/10
Descrição: Primeiramente, a equipa azul irá usar um Situational Awareness System (ISA), que permite mais facilmente acompanhar a pontuação, verificar como o exercício está a decorrer, e submeter os Situation Reports.
Para além disso, existirá um sistema de gestão de *injects*, no qual os participantes poderão ver e obter os *injects* dos monitores.
Existe também um sistema de tickets, no qual os organizadores conseguem obter notificações caso exista algum problema na infra estrutura do exercício.
Finalmente, existirá um servidor de mensagens, no qual os organizadores e a equipa azul poderão manter um contacto mais informal e rápido.

Definir monitores e observadores
Responsável: Organizador e equipa planeadora
Data-Limite: 03/10
Descrição:

Monitores:

- Coordenadores das unidades que participam no exercício

Observadores:

- Gestão de Topo
- Equipa de comunicação
- CNCS
- Rede Nacional de CSIRT

Definir metodologias de avaliação
Responsável: Equipa planeadora
Data-Limite: 03/10
Descrição:

O exercício será avaliado da seguinte forma para a equipa azul:

- Disponibilidade: Perdem pontos passivamente por cada máquina ou serviço que esteja inativo devido a um incidente e ganham pontos passivamente por cada máquina ativa
- Ataques: Perdem pontos se a equipa vermelha conseguir realizar um ataque com sucesso
- SITREP: Ganham pontos se entregarem o SITREP dentro do prazo e este contem conteúdo relevante e estrutura correta

Sempre que a equipa azul perde pontos, estes passam para a equipa vermelha.

Preparar Caderno de Participante e de Monitor
Responsável: Equipa planeadora
Data-Limite: 13/10
Descrição:

Tendo em conta a duração do exercício, este terá um formato mais simples.
O Caderno deverá conter as seguintes partes:

- Objetivo do exercício
- Atividades realizadas pelas equipas
- Objetivos de aprendizagem
- Horário dos acontecimentos (Briefing dos participantes, começo e fim do exercício, sessão de feedback)
- Introdução do cenário
- Critérios de avaliação

O Caderno de Monitor irá conter, adicionalmente aos pontos acima indicados, os *injects* e as fases do exercício.

Preparar questionário de avaliação
Responsável: Equipa planeadora
Data-Limite: 13/10
Descrição:

O questionário terá como objetivo dar voz aos participantes e pedir opinião sobre as temáticas do exercício. Podem conter perguntas sobre:

- Como avaliam o exercício e os *injects*?
- Foi útil para perceber as falhas que têm nas suas organizações?
- Foi acessível em termos de dificuldade e tempo?
- O espaço é adequado?

Treinar monitores e moderadores
Responsável: Equipa planeadora
Data-Limite: 10/10
Descrição: A sessão terá de abordar temáticas, tais como: qual a arquitetura do sistema que a equipa vermelha irá atacar e que a azul irá defender; qual o estado de maturidade de resposta a incidentes das universidades envolvidas; como mandarão os *injects* e quais os canais de comunicação; e a agenda do exercício.

Convidar participantes, observadores e media
Responsável: Equipa planeadora
Data-Limite: 04/10
Descrição: O convite pode ser de acordo com as preferências dos organizadores.

6.2.3 Decorrer do Exercício

Sessão inicial dos participantes
Responsável: Equipa planeadora
Data-Limite: 13/10
Descrição:

- Entrega de brindes e do caderno de participante.
- Explicação das regras do desafio.
- Explicação do ambiente e do cenário do exercício.

Executar o cenário e os *injects*
Responsável: Monitores
Data-Limite: 13/10
Descrição: Realizar os procedimentos de acordo com o planeado sub-subcapítulo 6.2.2.

Observar participantes e tirar notas, comparando com o cenário expectável e *checklists*
Responsável: Monitores
Data-Limite: 13/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.3, secção "Desenrolar do Exercício e sua Monitorização".

Relatar decisões dos participantes à equipa organizadora
Responsável: Monitores
Data-Limite: 13/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.3, secção "Desenrolar do Exercício e sua Monitorização".

6.2.4 Avaliação

Responder a questionários
Responsável: Participantes e Monitores
Data-Limite: 14/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Medir o Sucesso".

Compilar e avaliar resultados dos questionários e *feedback* dos monitores
Responsável: Equipa avaliadora
Data-Limite: 13/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Medir o Sucesso".

Preparar o relatório individual
Responsável: Equipa avaliadora
Data-Limite: 15/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Relatórios".

Preparar o relatório de grupo
Responsável: Equipa avaliadora
Data-Limite: 15/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Relatórios".

Preparar o relatório público
Responsável: Equipa avaliadora
Data-Limite: 15/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Relatórios".

Apresentar principais conclusões com os *stakeholders*
Responsável: Equipa avaliadora
Data-Limite: 16/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Medir o Sucesso".

Reunião futura de ponto de situação com os *stakeholders*
Responsável: Equipa avaliadora
Data-Limite: 21/10
Descrição: Realizar os procedimentos de acordo com o mencionado no subcapítulo 5.4, secção "Medir o Sucesso".

7 Experimentação e Avaliação

7.1 Hipótese

De modo que os exercícios desenvolvidos possam ser considerados como capazes de cumprir os seus objetivos, estes devem ser estudados quanto às seguintes hipóteses:

- Os exercícios criados ajustam-se ao contexto das IES;
- As equipas estão aptas para responder a ciberataques e incidentes de segurança.

7.2 Metodologia

Existem duas diferentes metodologias, uma para cada hipótese. Estas metodologias estarão apresentadas nos pontos seguintes.

7.2.1 Os exercícios criados ajustam-se ao contexto das IES

Para conseguir testar a primeira hipótese mencionada, será necessário recolher informação por parte dos participantes do exercício relativamente à proximidade do enunciado e arquitetura do cenário face à realidade. Isto pode ser feito através do questionário que lhes é dado no final do exercício. Isto é, cada participante avalia, por exemplo, cada *inject* de 1 a 10 de acordo com a sua proximidade ao contexto das IES e, se avaliar de 1 a 5 considera-se que não corresponde aos critérios da IES. Por outro lado, se avaliar de 6 a 10, considera-se que vai de acordo ao contexto da IES.

Para conseguir comparar estes valores, ter-se-á de partir do pressuposto que o sistema onde o exercício será executado tenha capacidade para criar e saber como criar, através de um *template* ou de uma biblioteca, *injects* adaptados à universidade. Cabe ao organizador do

exercício personalizar cada *inject* de acordo com a realidade da universidade dos participantes, de modo a ter resultados mais precisos.

Assim, criar-se-ão 3 exercícios, cada um com 10 *injects*, dos quais 8 são classificados como "adaptados ao contexto das IES" e 2 são classificados como "não adaptados ao contexto das IES". No fim de cada exercício, lança-se o questionário aos participantes, que terá como pergunta "Como classifica cada *inject* quanto ao contexto da sua IES?", e, depois dos participantes avaliarem numa escala de 1 a 10 cada *inject*, sendo 1 equivalente a "não vai de encontro ao contexto da IES" e 10 equivalente a "vai de encontro ao contexto da IES", e calcula-se a média das respostas em cada *inject,* de modo a obter a avaliação geral do mesmo.

Caso um *inject* não seja válido e um utilizador o marcar como não válido no contexto da IES, será tratado como um verdadeiro negativo (VN). Caso contrário, será tratado como um falso positivo (FP). Por outro lado, se o *inject* for criado de acordo com os parâmetros da IES e o utilizador o marcar como tal, será tratado como um verdadeiro positivo (VP). Caso contrário, será tratado como um falso negativo (FN). Esta informação está representada através da tabela 8.

Tabela 8 Matriz de classificação (Joshi, 2016)

	Injects que estão de acordo às necessidades da IES	*Injects* que não estão acordo às necessidades da IES	**TOTAL AVALIAÇÕES**
Participante marcou como válido	VP	FP	PP (totais marcados como válidos)
Participante marcou como não válido	FN	VN	PN (totais marcados como não válidos)
TOTAL CRIAÇÕES	OP (totais *injects* criados no contexto da IES)	ON (totais *injects* criados não no contexto da IES)	TOT

Ao compilar o *dataset* dos utilizadores, aplicar-se-á o modelo *K-fold cross validation*, que consiste em dividir os dados em K grupos e realizando K iterações de teste. Em cada iteração, utiliza-se um grupo de dados como sendo a amostra de teste e as restantes como amostra de treino.

Através do cálculo da exatidão é possível avaliar se o modelo consegue prever os dados. A exatidão pode ser calculada através da fórmula (5):

$$Acc = \frac{VP + VN}{TOT} \quad (5)$$

A precisão pode ser calculada através da fórmula (6) que, no contexto do exercício, responde à questão "De todos os *inject* classificados como válidos de acordo com as necessidades das IES, quantos é que realmente foram criados com esse intuito?" (Joshi, 2016):

$$Pre = \frac{VP}{PP} \tag{6}$$

A cobertura pode ser calculada através da fórmula (7) que, no contexto do exercício, responde à questão "De todos os *injects* criados de acordo com as necessidades das IES, quantos é que realmente foram classificados como tal?" (Joshi, 2016):

$$Rec = \frac{VP}{OP} \tag{7}$$

O *f1-score* pode ser calculado através da fórmula (8) que, no contexto do exercício, corresponde à média pesada da precisão e cobertura (Joshi, 2016):

$$F1 = \frac{2 * (Rec * Pre)}{(Rec + Pre)} \tag{8}$$

Considerar-se-á que o sistema consegue criar exercícios de acordo com o contexto das IES se o valor da exatidão (caso o mais importante seja os VP's e o VN) ou *f1-score* (caso o mais importante seja os FP's e o FN) for maior ou igual a 85%.

A título de exemplo, consideram-se os valores da tabela 9, para um total de 30 *injects*:

Tabela 9 Valores de exemplo para teste da primeira hipótese

	Injects que estão de acordo às necessidades da IES	*Injects* que não estão acordo às necessidades da IES	**TOTAL AVALIAÇÕES**
Participante marcou como válido	15	5	20
Participante marcou como não válido	9	1	10
TOTAL CRIAÇÕES	24	6	30

Com estes valores, obtém se que a exatidão é 0.53, a precisão é 0.75, a cobertura é 0.625 e, por conseguinte, o *f1-score* equivale a 0.68, implicando que, com estes valores, os exercícios criados não estão de acordo ao contexto das IES, visto que a meta seria o *f1-score* ou a exatidão serem iguais ou superiores a 0.85.

7.2.2 As equipas estão aptas para responder a ciberataques e incidentes de segurança

Para conseguir testar a segunda hipótese mencionada na secção 7.1, foram definidos testes estatísticos que futuramente serão aplicados à medida que os exercícios vão acontecendo. Desta forma, inicializou-se esta análise com a definição das variáveis que é possível obter no início e no final de um ciberexercício. Tendo em conta estas variáveis, é possível identificar qual o tipo de dado dessa variável e que possíveis relações podem ter com outras variáveis ou circunstâncias. Esta informação encontra-se compilada na tabela 10.

Tabela 10 Variáveis para avaliar ciberexercícios

Variável	Tipo de Dados	Relações	Método de Recolha
Autoavaliação do participante quanto à capacidade de resposta a incidentes de segurança	Intervalo 1-10	*Hints* usadas (só aplicável ao pré exercício)	Questionário de participante (pré- e pós-exercício)
Downtime das máquinas	Tempo em minutos	Em que universidade o exercício foi realizado	Sistema automático de pontuação
Comprometimento das máquinas	Tempo em minutos	Em que universidade o exercício foi realizado	Sistema automático de pontuação
Número de ataques realizados às várias zonas da infraestrutura	Numérico	Em que universidade o exercício foi realizado	Sistema automático de pontuação
Hints usadas	Numérico	- Autoavaliação da equipa quanto à capacidade de resposta a incidentes de segurança (pré-exercício); - Passos expectados foram cumpridos	Sistema automático de pontuação
Desempenho no exercício	Intervalo 1-10	Número do exercício	Avaliação dos monitores
Nota de cada *Situational Report*	Intervalo 1-10	Número do exercício	Avaliação dos monitores

De seguida, procedeu-se à definição do teste estatístico para cada variável estudada.

Autoavaliação dos participantes

Será criada a variável "Autoavaliação do participante", que representa a avaliação que cada participante dá ao que considera ser a sua capacidade de responder a incidentes de segurança.

Através de um questionário entregue no início e final do ciberexercício, o participante indica esta variável através de uma classificação de 1 a 10. Neste caso, pretende-se verificar que se existe diferença estatisticamente significativa nesta perspetiva no início e final do exercício.

Para isso, criar-se-á um exercício e colecionar-se-á as autoavaliações tanto no início como no final do exercício, nas quais será verificada a normalidade dos resultados através do teste de Shapiro-Wilk. Como estão em estudo 2 variáveis (sendo uma qualitativa – antes ou depois do exercício – e outra quantitativa – nota de autoavaliação) e como está em estudo 2 grupo (pré- e pós-exercício), se estas seguirem uma distribuição normal, aplicar-se-á o teste Student t-test para amostras emparelhadas. Se não, aplicar-se-á o teste Wilcoxon.

Downtime das máquinas

É criada a variável "*Downtime* das máquinas", que representa o tempo, em minutos, que cada máquina se encontra desativada. O valor para cada máquina é recolhido no sistema automático de pontuação. Neste caso, pretende-se verificar se existe diferença estatisticamente significativa no tempo de *downtime* das máquinas de um exercício em cada universidade onde o exercício decorre. É de notar que este teste só é possível ser realizado em exercícios *live-play.*

Para isso, criar-se-á um exercício que irá ser replicado em circunstâncias semelhantes em 5 universidades e registar-se-á o tempo que cada máquina do exercício se encontra desativada. Depois de registados estes tempos de cada máquina, verificar-se-á a normalidade dos resultados através de um teste Shapiro-Wilk. Como estão em estudo 2 variáveis independentes (sendo uma qualitativa – nome da universidade – e outra quantitativa – tempo de cada máquina) e como está em estudo mais que 2 grupos (cada universidade é um grupo), se estas seguirem uma distribuição normal, aplicar-se-á o teste ANOVA. Se não, aplicar-se-á o teste Kruskal-Wallis.

Comprometimento das máquinas

É criada a variável "Comprometimento das máquinas", que representa o tempo, em minutos, que cada máquina se encontra comprometida. O valor para cada máquina é recolhido no sistema automático de pontuação. Neste caso, pretende-se verificar se existe diferença estatisticamente significativa no tempo de comprometimento das máquinas de um exercício em cada universidade onde o exercício decorrer. É de notar que este teste só é possível ser realizado em exercícios *live-play.*

Para isso, criar-se-á um exercício que irá ser replicado em circunstâncias semelhantes em 5 universidades e registar-se-á o tempo que cada máquina do exercício se encontra comprometida. Depois de registados estes tempos de cada máquina, verificar-se-á a normalidade dos resultados através de um teste Shapiro-Wilk. Como estão em estudo 2 variáveis independentes (sendo uma qualitativa – nome da universidade – e outra quantitativa – tempo de cada máquina) e como está em estudo mais que 2 grupos (cada universidade é um grupo), se estas seguirem uma distribuição normal, aplicar-se-á o teste ANOVA. Se não, aplicar-se-á o teste Kruskal-Wallis.

Número de Ataques

É criada a variável "Número de ataques", que representa o número de ataques realizados a um grupo de máquinas. Neste contexto, a palavra grupo refere-se a cada pequena infraestrutura de máquinas dentro de um exercício, que pode ser, por exemplo, os servidores de infraestrutura crítica ou os computadores de uma sala em particular. O valor para cada grupo é recolhido no sistema automático de pontuação. Neste caso, pretende-se verificar se existe diferença estatisticamente significativa no número de ataques realizados em cada grupo e em cada universidade. É de notar que este teste só é possível ser realizado em exercícios *live-play*.

Para isso, criar-se-á um exercício que irá ser replicado em circunstâncias semelhantes em 5 universidades e registar-se-á o número de ataques em cada grupo. Depois de registados estes ataques, verificar-se-á a normalidade dos resultados através de um teste Shapiro-Wilk. Como estão em estudo 2 variáveis independentes (sendo uma qualitativa – nome da universidade – e outra quantitativa – número de ataques) e como está em estudo mais que 2 grupos (cada universidade é um grupo estatístico), se estas seguirem uma distribuição normal, aplicar-se-á o teste ANOVA. Se não, aplicar-se-á o teste Kruskal-Wallis.

Hints utilizadas

É criada a variável "*Hints* utilizadas", que representa o número de *hints* ou dicas que uma equipa usou num determinado exercício. Neste caso, pretende-se verificar se existe correlação entre esta variável e a autoavaliação média que os participantes da equipa indicou.

Para isso, criar-se-á três exercícios distintos que irão ser realizados na mesmo universidade ao longo de um determinado período. Em cada exercício, registar-se-á o número de *hints* utilizadas por equipa e a média da autoavaliação dos participantes da equipa relativa às suas capacidades. Depois de registados estes valores, verificar-se-á a normalidade dos resultados através de um teste Shapiro-Wilk. Como estão em estudo 2 variáveis independentes (sendo as duas quantitativas – número de dicas e valor da autoavaliação), se estas seguirem uma distribuição normal, aplicar-se-á a correlação de Pearson. Se não, aplicar-se-á a correlação de Spearman.

Para além deste caso, pretende-se também se verificar se existe correlação entre esta variável e a percentagem de sucesso que a equipa obteve em realizar os passos para completar o exercício, de acordo com o cenário expectável e a solução do exercício. Para isso, criar-se-á três exercícios distintos que irão ser realizados na mesmo universidade ao longo de um determinado período. Em cada exercício, registar-se-á o número de *hints* utilizadas por equipa e a percentagem de passos realizados. Depois de registados estes valores, verificar-se-á a normalidade dos resultados através de um teste Shapiro-Wilk. Como estão em estudo 2 variáveis independentes (sendo as duas quantitativas – número de dicas e valor da percentagem), se estas seguirem uma distribuição normal, aplicar-se-á a correlação de Pearson. Se não, aplicar-se-á a correlação de Spearman.

Desempenho no Exercício

É criada a variável "Desempenho individual", que representa a avaliação global que o monitor dá à equipa. Neste caso, pretende-se verificar se existe diferença estatisticamente significativa neste desempenho ao longo do tempo e ao longo que os exercícios decorrem. É de notar que este teste só é possível ser realizado em exercícios *live-play.*

Para isso, criar-se-á dois exercícios numa universidade, nos quais os monitores registarão o desempenho individual de cada participante. Depois de registados estes ataques, verificar-se-á a normalidade dos resultados através de um teste Shapiro-Wilk. Como estão em estudo 2 variáveis (sendo uma qualitativa – identificador do exercício – e outra quantitativa – nota de autoavaliação) e como está em estudo 2 grupos (exercício 1 ou 2), se estas seguirem uma distribuição normal, aplicar-se-á o teste Student t-test para amostras emparelhadas. Se não, aplicar-se-á o teste Wilcoxon.

Nota Situational Report

É criada a variável "Classificação Situational Report", que representa a classificação que é dada pelo monitor, de 1 a 5, a cada relatório entregue num exercício pela equipa azul. Neste caso, pretende-se verificar se existe diferença estatisticamente significativa nas classificações ao longo do tempo e ao longo que os exercícios decorrem.

Para isso, criar-se-á três exercícios diferente que irão ser realizados numa universidade e registar-se-á a classificação em cada Situational Report. Depois de registados estes valores, verificar-se-á a normalidade dos resultados através de um teste Shapiro-Wilk. Como estão em estudo 2 variáveis independentes (sendo uma qualitativa – identificador do exercício – e outra quantitativa – classificação do relatório) e como está em estudo mais que 2 grupos (cada exercício é um grupo estatístico), se estas seguirem uma distribuição normal, aplicar-se-á o teste ANOVA. Se não, aplicar-se-á o teste Kruskal-Wallis.

8 Conclusão

Este documento tinha como objetivo inicial analisar as componentes do CyberLab prévias à implementação da solução. Contudo, esse objetivo ultimamente mudou, visto que o projeto não avançou no ritmo expectável, tornando assim inviável conseguir cumprir os objetivos inicialmente estabelecidos nesse âmbito. Dessa forma, surgiu-se a necessidade de diferenciar o que eram os objetivos originalmente do projeto e quais eram os objetivos que este trabalho visava cumprir. Decidiu-se, assim, que o objetivo do trabalho seria fornecer ao leitor um guião de como planear, executar e avaliar um ciberexercício no âmbito e contexto de uma IES. Isto teria como objetivo o conseguir adaptar esse guião e esses ensinamentos à plataforma que futuramente viria ser adquirida, de modo a ter mais antecipadamente o *know-how* de como criar estes exercícios.

Comprovou-se a necessidade crescente de investir na cibersegurança na área de Ensino Superior em Portugal. As equipas que fazem parte dos serviços administrativos da universidade necessitam de mais e melhor sensibilização para a temática e mais frequentes exercícios e treino para conseguir lidar com os vários incidentes dos dias de hoje. Ao apresentar o guião de planeamento de exercícios, os dois exemplos mencionados, e a metodologia de avaliar o estado da aptidão e capacidade das equipas e da criação dos ciberexercícios, fornece-se um base de ferramentas e materiais para se iniciar o processo de implementar esta cultura de cibersegurança nas universidades portuguesas e, eventualmente, em mais áreas da Administração Pública.

Entendeu-se que o processo de criar um exercício envolve, para além do conhecimento técnico, várias áreas de logística, comunicação, e relações interinstitucionais, pelo que a realização dos exemplos dos exercícios permitiu ter alguma experiência prática em como planear estes cenários e simulações nas universidades.

8.1 Progressão temporal das tarefas

O trabalho necessitou de bases teóricas e de literatura. Tendo em conta que a criação dos cenários e exercícios de acordo com as necessidades das IES e da AP são dos pontos mais essenciais, considerou-se relevante investigar sobre a composição, estrutura e tipologia dos ciberexercícios, nos quais se colecionou informação sobre o ciclo de vida dos mesmos e sobre as características de Cyber Range, CTF, e Threat Hunting. Para além disso, de forma a criar uma solução confiável e que segue as principais normas e modelos de cibersegurança, investigou-se e apresentou-se informação sobre algumas das principais normas em vigor tanto a nível europeu ou norte-americano. Nomeadamente, compilou-se os requisitos, características, e fundamentos das normas NIST NICE Cybersecurity Workforce Framework, NIST Framework, a Diretiva NIS, o MITRE ATT&CK e a família de normas ISO 27000, dando especial atenção à ISO 27001.

De forma a entender e relatar qual a principal proposta de valor do projeto, realizou-se uma análise aos requisitos e necessidades do mesmo. Foi relatado como foi possível alcançar o estado atual de desenvolvimento partindo da identificação a necessidade e oportunidade de o desenvolver. Também foi definido o modelo CANVAS e análise SWOT como metodologias e planeamento estratégico e definição da proposta de valor do projeto. Finalmente, foram construídos e realizados dois modelos para auxílio à decisão estratégica de desenvolvimento: o QFD e o TOPSIS:

- O primeiro teve como objetivo definir quais os requisitos do cliente e critérios de engenharia com mais peso, no qual se concluiu que os requisitos mais importantes eram o da criação e realização de cenários de cibersegurança, incluindo interfaces próprias para as diferentes equipas envolventes. Também foi concluído que o critério mais importante para o sucesso do projeto seria a qualidade dos algoritmos de criação de ciberexercícios e de monotorização e pontuação dos mesmos;
- O segundo destacou-se pela capacidade de ajudar a determinar qual a solução existente mais próxima do ideal, a qual, de acordo com os valores inseridos, a da CyberExer foi classificada com a mais próxima e ajustada às necessidades do CyberLab.

De seguida, originalmente, foram compiladas e organizadas a métricas idealizadas no contexto de avaliação do projeto. A partir destas métricas, foram idealizadas as hipóteses nulas e testes estatísticos a realizar em cada caso.

Na segunda parte do trabalho, foi desenvolvido o corpo principal do documento. Foram compiladas informações de alguns guiões de planeamento de um ciberexercício, de maneira a criar um guião de como executar este planeamento. Este guião passou por vários aspetos deste processo de criação, desde os benefícios do exercício, à seleção do espaço, planeamento das reuniões, elaboração de relatórios, identificação de objetivos, entre outros.

Depois de realizado este guião, utilizou-se os conhecimentos adquiridos para criar dois exemplos de ciberexercícios. O primeiro consistiu num exercício *tabletop,* com a duração de algumas horas, no qual se simulou que uma universidade estaria a ser atacada por um Lockbit

Ransomware. Em contrapartida, o segundo exercício consistiu num *live-play*, onde se simulou uma competição entre uma equipa atacante e uma defensora, apresentando um maior nível de detalhe, incluindo um diagrama da arquitetura. Estes exemplos fizeram-se acompanhar de um progresso detalhado dos vários passos que englobam este planeamento, desde à sua conceção até à fase final do ciberexercício.

Sabendo que é possível obter várias métricas e variáveis antes e após o decorrer do exercício, as métricas e testes estatísticos previamente escritos foram atualizados para englobar estas alterações. Para além de ter sido reformulado ligeiramente a primeira hipótese de teste, a segunda hipótese nula consistiu em verificar se os participantes se encontrariam realmente aptos para responder a incidentes de segurança.

8.2 Limitações

O desenvolvimento deste relatório abrangeu diversas limitações que impediram a demonstração de resultados mais acertados e precisos. Das mais significativas, destacam-se:

- O projeto não ter progredido no ritmo expectável, pelo que não existe nenhum programa onde seja possível criar, na prática, os exercícios propostos;
- Devido ao ponto anterior, os resultados dos modelos QFD e TOPSIS, assim como as listas de requisitos e critérios presentes no mesmo, podem não corresponder na totalidade à situação real do projeto, pelo que estes valores podem futuramente serem acertados consoante os ajustes definidos na implementação da solução;
- Finalmente, não foi possível utilizar dados reais para exemplificar e demonstrar resultados dos testes estatísticos e métricas definidas.

8.3 Trabalho Futuro

Quando for o momento apropriado para iniciar os desenvolvimentos dos ciberexercícios, este documento poderá ser usado como base, referência e exemplo para criar os exercícios, de maneira que sejam adaptados ao contexto das IES. Para além disso, os resultados presentes no documento servirão como uma referência para que algumas das principais questões do projeto sejam alinhadas e, de igual forma, para proporcionar modelos desenhados que auxiliarão este desenvolvimento. A título de exemplo, através do trabalho realizado nos modelos TOPSIS e QFD, torna-se possível alcançar uma resposta mais rápida às questões que estes pretendem responder, pelo que só é necessário inserir os valores mais ajustados às necessidades do cliente. Ademais, a compilação dos testes estatísticos a partir das métricas ajuda a tornar mais simples a futura realização e preenchimento destas metodologias de avaliação quando os dados estiverem na posse da equipa desenvolvedora. Espera-se, assim, que nas implementações futuras dos exercícios, a adaptação a esta cultura e a implementação de um *know-how* mais aprofundado da cultura de ciberexercícios seja mais facilitada e ágil.

Referências

2021. Capture-The-Flag Competitions: all you ever wanted to know! *ENISA News*.

ACHIAGA, M. D. M. N. 2022. A Europe Fit for the Digital Age. *Review of the Directive on security of network and information systems.* europarl.europa.eu: European Parliment.

AKAO, Y. 1990. *Quality Function Development: Integrating Customer Requirements into Product Design*.

BEHAVIOUR 2017. Schedule for Day 1. *ISO/IEC 27001 ISMS Training.* Behaviour.

CNCS - CENTRO NACIONAL DE CIBER SEGURANÇA 2019. Quadro Nacional de Referência para a Cibersegurança. CNCS - Centro Nacional de Ciber Segurança.

CNCS - CENTRO NACIONAL DE CIBERSEGURANÇA 2021. Relatório Cibersegurança em Portugal - Riscos e Conflitos.

CYBERBIT. 2022. *Cyberbit – Cyber Range Platform leading provider* [Online]. Available: https://www.cyberbit.com/ [Accessed 18-Feb 2022].

CYBEREXER. 2021. *What is a Cyber Range* [Online]. CyberExer. Available: https://www.cybexer.com/products/cyber-range [Accessed 01-Jan 2022].

DEWULF, K. 2012. Sustainable Product Innovation: The Importance of the Front-End Stage in the Innovation Process.

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY. *NIS Directive* [Online]. Available: https://www.enisa.europa.eu/topics/nis-directive?tab=details [Accessed 13-Feb. 2022].

ENISA - EUROPEAN UNION AGENCY FOR CYBERSECURITY 2009. Good Practice Guide on National Exercises.

EUROPEAN UNION 2016. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. EUR-Lex: Official Journal of the European Union.

GRANÅSEN, M. & ANDERSSON, D. 2016. Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. *Cognition, Technology & Work,* 18**,** 121-121-143.

HACKEDU. *What is a Capture The Flag Event, and How Does It Benefit Developers?* [Online]. Available: https://www.hackedu.com/blog/what-is-a-capture-the-flag-ctf-event-and-how-can-it-benefit-developers [Accessed 13-Feb 2022].

HENRY, J. 2019. *10 Reasons Cyber Range Simulation Is Vital to Incident Response* [Online]. Available: https://securityintelligence.com/articles/10-reasons-cyber-range-simulation-is-vital-to-incident-response/ [Accessed 13-Feb 2022].

IBM. *What is threat hunting?* [Online]. IBM. Available: https://www.ibm.com/se-en/topics/threat-hunting [Accessed 02-Jan 2022].

INTEGRITY. 2022. *ISO 27001* [Online]. Available: https://www.27001.pt/ [Accessed 13-Feb 2022].

JOSHI, R. 2016. *Accuracy, Precision, Recall & F1 Score: Interpretation of Performance Measures - Exsilio Blog* [Online]. Available: https://blog.exsilio.com/all/accuracy-precision-recall-f1-score-interpretation-of-performance-measures/ [Accessed 20-Feb. 2022].

KARJALAINEN, M., KOKKONEN, T. & PUUSKA, S. 2019. Pedagogical Aspects of Cyber Security Exercises.

KIM, G., PARK, C. S. & YOON, K. P. 1997. Identifying investment opportunities for advanced manufacturing systems with comparative-integrated performance measurement. *International Journal of Production Economics,* 50**,** 23-23 - 33.

KOSUTIC, D. *ISO 27001 checklist: 16 steps for the implementation* [Online]. Advisera: 27001academy. Available: https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/ [Accessed 13-Feb. 2022].

MCAFEE. *What Is the MITRE ATT&CK Framework?* [Online]. McAfee. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html [Accessed 02-Jan 2022].

NATIONAL CYBER SECURITY CENTRE 2020. Effective steps to cyber exercise creation.

NEGREIRO, M. 2021. The NIS2 Directive: A high common level of cybersecurity in the EU. *In:* SERVICE, M. R. (ed.). europarl.europa.eu: European Parliament.

NINA WILHELMSON, T. S. 2011. Handbook for planning, running and evaluating information technology and cyber security exercises. Swedish Defence University, CATS (Center for Asymmetric Threat Studies).

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2018. Framework for Improving Critical Infrastructure Cybersecurity.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2020. Workforce Framework for Cybersecurity (NICE Framework)

OŠLEJŠEK, R., VYKOPALY, J., BURSKÁ, K. & RUSˇNÁK, V. 2018. Evaluation of Cyber Defense Exercises Using Visual Analytics Process.

QUALIDADE, I. P. D. 2013. Norma Portuguesa ISO/IEC 27001.

ŞEKER, E. 2019. The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation.

SHIH, H.-S., SHYUR, H.-J. & LEE, E. S. 2007. An extension of TOPSIS for group decision making.

SKOWRON, M. 2020. *Lean Canvas vs Business Model Canvas: Which Should You Choose?* [Online]. UIG Studio. Available: https://uigstudio.com/insights/lean-canvas-vs-business-model-canvas-which-should-you-choose [Accessed 02-Jan 2022].

TASCHLER, S. 2021. *WHAT IS CYBER THREAT HUNTING?* [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/threat-hunting/ [Accessed 02-Jan 2022].

TAYLOR, H. 2021. *What is a cyber range?* [Online]. CyberSecurity Guide. Available: https://cybersecurityguide.org/resources/cyber-ranges/ [Accessed 01-Jan 2022].

TRAFICOM - FINNISH TRANSPORT AND COMMUNICATIONS AGENCY 2020. Instructions for organising cyber exercises.

UNIVERSIDADE DE AVEIRO, UNIVERSIDADE DO PORTO & UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO 2019. CYBERLAB - CYBERSECURITY INNOVATION LAB FOR PUBLIC ADMINISTRATION. *SISTEMA DE APOIO À MODERNIZAÇÃO E CAPACITAÇÃO DA ADMINISTRAÇÃO PÚBLICA (SAMA 2020)*.

VICTORIA STATE GOVERNMENT 2019. A guide to cyber exercises.

WU, S. M., YOU, X. Y., LIU, H. C. & WANG, L. E. 2020. Improving quality function deployment analysis with the cloud MULTIMOORA method. *International Transactions in Operational Research,* 27**,** 1600-1621.

Anexo A – Tabela MITRE ATT&CK

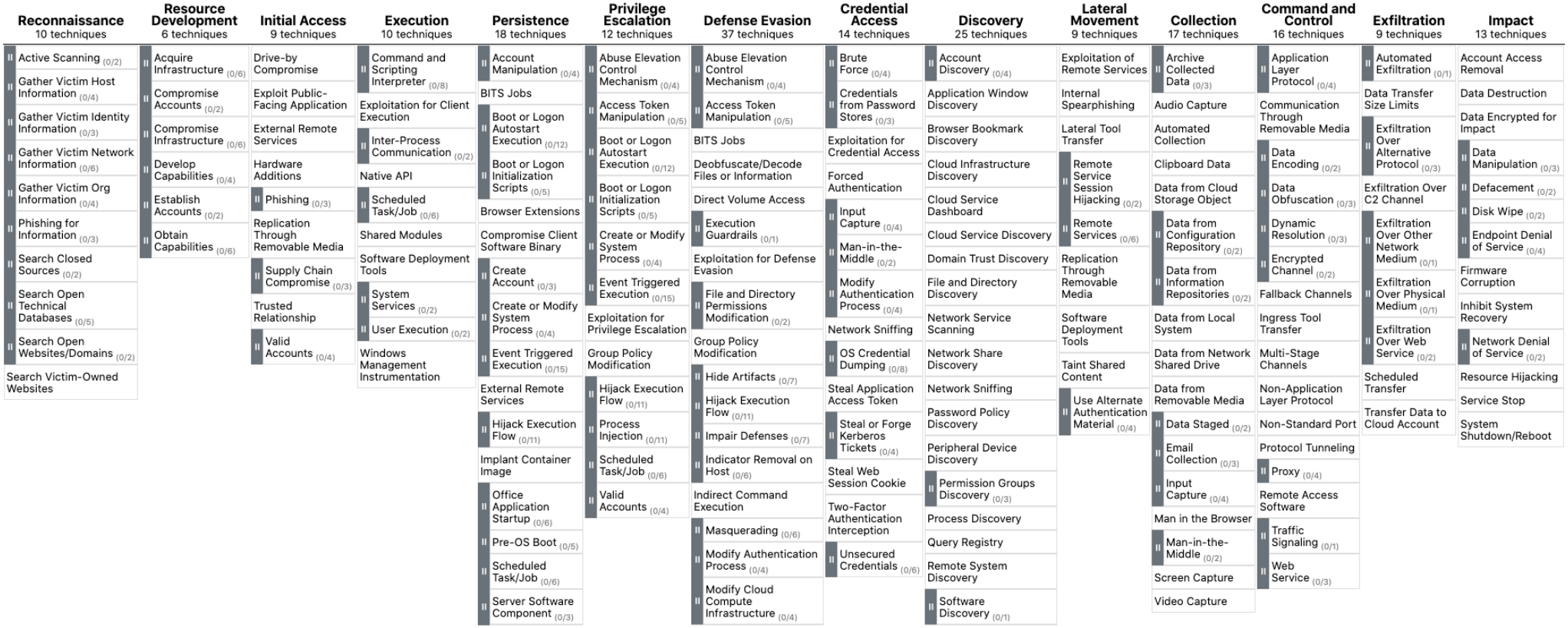

Figura 7 Tabela MITRE ATT&CK

Anexo B – Tabela da Folha de Cálculo do TOPSIS

Matriz ^2										
Empresas\Critérios	Qtd. Utilizadores	Qual. Exer. CyberRange	Qual. Exer. CTF	Qual. Exer. Conjunto	Auto-aprendizagem	Qual. Algoritmo Criação de Exer.	Monotorização	Sistema de Pontuação	Manutenção (Auditorias, atualizações)	Testagem de Modelos Operacionais
CyberExer	100	100	81	36	64	81	36	49	64	0
CyberBit	49	64	0	81	81	49	64	49	100	0
Soma	149	164	81	117	145	130	100	98	164	0
RAIZQSOMA	12.20655562	12.80624847	9	10.81665383	12.04159458	11.40175425	10	9.899494937	12.80624847	0

Figura 8 Matriz da raiz quadrática da soma dos quadrados de cada fator

Matriz Normalizada pesada										
Empresas\Critérios	Qtd. Utilizadores	Qual. Exer. CyberRange	Qual. Exer. CTF	Qual. Exer. Conjunto	Auto-aprendizagem	Qual. Algoritmo Criação de Exer.	Monotorização	Sistema de Pontuação	Manutenção (Auditorias, atualizações)	Testagem de Modelos Operacionais
CyberExer	122.0655562	128.0624847	81	64.89992296	96.33275663	102.6157883	60	69.29646456	102.4499878	0
CyberBit	85.44588931	102.4499878	0	97.34988444	108.3743512	79.81227976	80	69.29646456	128.0624847	0

Figura 9 Matriz normalizada pesada

Multiplicar cada elemento da matriz pelo peso da respectiva coluna										
Empresas\Critérios	Qtd. Utilizadores	Qual. Exer. CyberRange	Qual. Exer. CTF	Qual. Exer. Conjunto	Auto-aprendizagem	Qual. Algoritmo Criação de Exer.	Monotorização	Sistema de Pontuação	Manutenção (Auditorias, atualizações)	Testagem de Modelos Operacionais
CyberExer	3.785324792	13.20800746	8.354114062	2.910990497	5.807408795	24.0011633	4.570552422	6.578858597	16.09890601	0
CyberBit	2.649727354	10.56640597	0	4.366485746	6.533334894	18.66757145	6.094069897	6.578858597	20.12363251	0

Figura 10 Multiplicação de cada célula pelo peso do respetivo fator

Separação da solução ideal positiva												
Empresas\Critérios	Qtd. Utilizadores	Qual. Exer. CyberRange	Qual. Exer. CTF	Qual. Exer. Conjunto	Auto-aprendizagem	Qual. Algoritmo Criação de Exer.	Monotorização	Sistema de Pontuação	Manutenção (Auditorias, atualizações)	Testagem de Modelos	SOMA	Si
CyberExer	0	0	0	2.118466419	0.526968702	0	2.321105494	0	16.19842342	0	21.16496403	4.60053954
CyberBit	1.28958154	6.978058448	69.79122176	0	0	28.44720195	0	0	0	0	106.5060637	10.3201775

Figura 11 Separação da solução ideal positiva

Separação da solução ideal negativa												
Empresas\Critérios	Qtd. Utilizadores	Qual. Exer. CyberRange	Qual. Exer. CTF	Qual. Exer. Conjunto	Auto-aprendizagem	Qual. Algoritmo Criação de Exer.	Monotorização	Sistema de Pontuação	Manutenção (Auditorias, atualizações)	Testagem de Modelos	SOMA	Si
CyberExer	1.28958154	6.978058448	69.79122176	0	0	28.44720195	0	0	0	0	106.5060637	10.3201775
CyberBit	0	0	0	2.118466419	0.526968702	0	2.321105494	0	16.19842342	0	21.16496403	4.60053954

Figura 12 Separação da solução ideal negativa

Cálculo da proximidade relativa à solução ideal Ci* = S'i / (Si* +S'i)	
CyberExer	0.691667664
CyberBit	0.308332336

Figura 13 Cálculo da proximidade à solução ideal

Anexo C – Checklist de Planeamento de Ciberexercícios

Tabela 11 Checklist de Planeamento de Ciberexercícios

Data	Completo	Tarefa	Responsável
Identificação do Exercício			
		Identificar objetivo do exercício	Organizador
		Identificar participantes	Organizador
		Identificar tipo de exercício	Organizador
		Identificar stakeholders	Organizador
Planeamento			
		Realizar esquema e objetivos de futuras reuniões	Organizador
		Definir data e local do exercício	Organizador e equipa planeadora
		Preparar *injects* e enunciados do exercício	Equipa planeadora
		Definir agenda do evento	Organizador e equipa planeadora
		Definir canais de comunicação	Organizador e equipa planeadora
		Definir monitores e observadores	Organizador e equipa planeadora
		Definir metodologias de avaliação	Equipa planeadora
		Preparar Caderno de Participante e de Monitor	Equipa planeadora
		Preparar questionário de avaliação	Equipa planeadora
		Treinar monitores e moderadores	Equipa planeadora
		Convidar participantes, observadores e media	Equipa planeadora
Decorrer do Exercício			
		Sessão inicial dos participantes	Equipa planeadora
		Executar o cenário e os injects	Monitores
		Observar participantes e tirar notas, comparando com o cenário expectável e *checklists*	Monitores
		Relatar decisões dos participantes à equipa organizadora	Monitores

Data	Completo	Tarefa	Responsável
Avaliação			
		Responder a questionários	Participantes e Monitores
		Compilar e avaliar resultados dos questionários e feedback dos monitores	Equipa avaliadora
		Preparar o relatório individual	Equipa avaliadora
		Preparar o relatório de grupo	Equipa avaliadora
		Preparar o relatório público	Equipa avaliadora
		Apresentar principais conclusões com os *stakeholders*	Equipa avaliadora
		Reunião futura de ponto de situação com os *stakeholders*	Equipa avaliadora