Framework de recomendações e boas práticas orientada às Instituições de Ensino

(Agrupamento de Escolas/Escolas Não Agrupadas)

Proposta para projeto de Mestrado de Cibersegurança e Informática Forense

Filipe Bagagem
Politécnico de Leiria
Leiria, Portugal
2220558@my.ipleiria.pt

***Resumo*—Com a digitalização, as instituições de ensino estão cada vez mais vulneráveis a ciberataques, o que pode comprometer a confidencialidade, a integridade e a disponibilidade dos dados dos utentes/ex-utentes (alunos, docentes, não docentes e colaboradores) e causar sérios prejuízos financeiros e reputacionais. A Framework de recomendações e boas práticas a desenvolver é para auxiliar os Agrupamentos de Escolas e Escolas não Agrupadas Portuguesas na gestão, resposta e tratamento de incidentes de cibersegurança.**

***Index Terms*—incidentes, boas práticas, cibersegurança.**

I. Introdução

A cibersegurança é um tema cada vez mais importante e presente no mundo digital em que vivemos. As instituições de ensino, tanto públicas quanto privadas, com a disponibilização de vários serviços para a Internet estão sujeitas a ciberataques que podem comprometer a segurança de dados sensíveis, como informações dos utentes/ex-utentes (alunos, docentes, não docentes e colaboradores), registos académicos e financeiros. É fundamental que estas instituições de ensino estejam preparadas e tenham medidas de segurança adequadas para proteger os seus dados e a própria infraestrutura contra ciberataques. Neste contexto, a presente proposta tem como objetivo preparar uma framework de recomendações e boas práticas orientada aos Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) de Portugal. O Agrupamento de Escolas (AE) é uma unidade organizacional, dotada de órgãos próprios de administração e gestão, constituída por estabelecimentos de educação pré-escolar e escolas de um ou mais níveis e ciclos de ensino. A definição de uma Escola não Agrupada (ENA) é um estabelecimento de ensino, não superior, que não integra em agrupamento de escolas. De momento, existem 809 Unidades Orgânicas (AE e ENA), e 5540 Estabelecimentos de Ensino Públicos do Ensino Pré-Escolar, Básico e Secundário.

A. Descrição do Problema

O aumento da utilização de tecnologias em instituições de ensino tem levado a um crescente número de incidentes de cibersegurança, que podem ter impacto na integridade, confidencialidade e disponibilidade dos sistemas e dados. De acordo com um relatório recente da Sophos - "The State of Ransomware in Education 2022", as instituições de ensino estão a ser cada vez mais atingidas por ataques de ransomware. Em concreto, 60% estabelecimentos, quer de educação superior, quer secundária e básica, sofreram ataques em 2021, comparativamente a 2020 – 40"As escolas estão entre as instituições mais atingidas por ransomware, sendo alvos preferenciais para os atacantes devido à falta generalizada de defesas de cibersegurança sólidas e à 'mina de ouro' de dados pessoais que possuem", afirmou Chester Wisniewski, Principal Research Scientist da Sophos.

A precessão que disponho no momento, é que os AE/ENA Portuguesas não estão preparadas para enfrentar esta nova realidade do cibercrime, pelas seguintes razões:

- 1 - Infraestrutura tecnológica
  De uma forma geral, a infraestrutura tecnológica é um elemento importante nas instituições de ensino, pois possibilita uma série de benefícios para toda a comunidade escolar. Numa área cada vez mais digital, é importante ter acesso a recursos tecnológicos para melhorar o ensino e a aprendizagem. No entanto, a implementação de uma infraestrutura tecnológica de qualidade requer um investimento significativo em recursos tecnológicos e humanos, o que pode ser um desafio para muitas instituições de ensino. Além disso, é importante que a tecnologia seja utilizada de forma adequada e responsável, evitando problemas relacionados com a segurança de dados e a privacidade.

  1.1 - Ausência de planos de cópias de segurança
  A ausência de planos de cópias de segurança pode levar a graves consequências, como perda de dados críticos ou sensíveis das instituições de ensino. Sem planos adequados de backup, os dados podem ser perdidos para sempre em caso de falhas técnicas, erro humano, desastres naturais, ciberataques e outros eventos imprevistos. Na maioria dos AE/ENA não existe um plano de cópias de segurança e/ou mecanismo em uso não são seguros.

  1.2 - Infraestrutura ao nível da rede
  Na maioria dos AE /ENA têm ao ser dispor a rede minedu, trata-se de uma infraestrutura de rede a nível na-

cional que o Ministério da Educação criou para servir as instituições de ensino. Atualmente, há vários problemas na infraestrutura de rede que estão afetar a qualidade do serviço de comunicações nas instituições de ensino, tais como: Equipamentos desatualizados e com vários anos de uso, a baixa largura de banda que prejudica o desempenho de acesso a ferramentas online e o acesso a conteúdos alojados nas próprias instalações das instituições de ensino.

1.3 - Infraestrutura ao nível dos servidores

Os servidores devem ser configurados de forma a garantir a segurança da informação que armazenam e disponibilizam para a intranet e internet. Devem conter apenas software atualizado e licenciado, sistemas de backup e redundância para garantir a continuidade dos serviços em caso de falha. Os servidores devem ser constantemente monitorizados, para garantir a segurança dos sistemas e dos dados da instituição de ensino. Na maioria dos AE/ENA os servidores que disponibilizam serviços à comunidade escolar já estão obsoletos e não são monitorizados.

- 2 - Recursos humanos na área de cibersegurança
  A falta de recursos humanos de cibersegurança nas instituições de ensino é um problema crescente e alarmante. Com o aumento constante de ciberataques, as instituições de ensino são frequentemente alvo de ciberataques. Embora as instituições de ensino estejam cientes dos riscos associados aos ciberataques, elas enfrentam dificuldades em recrutar profissionais qualificados de cibersegurança. Atualmente, a procura de profissionais de cibersegurança excede a oferta, e a ausência de salários competitivos nestas instituições de ensino, não atrai estes profissionais. A falta de consciencialização sobre a importância da cibersegurança é outro fator que deve ser tido em conta, é necessário treinar todos os recursos humanos das instituições de ensino (alunos, docentes e não docentes) para criar uma cultura de cibersegurança.
- 3 - Plano de Resposta a Incidentes
  Um plano de resposta a incidentes é fundamental para garantir a segurança das pessoas e a continuidade das atividades educativas em caso de um ciberataque. As instituições de ensino devem ter um plano bem definido e que seja atualizado regularmente, com todas as diretrizes e procedimentos adotar em situações de emergência. Na maioria dos AE/ENA não existe um plano de resposta a incidentes e muitos não sabem do que se trata.
- 4 - Política de utilização Aceitável (PUA)
  Na maioria dos AE/ENA não existe uma política de utilização aceitável ou nos casos em que existe a mesma não se encontra atualizada. A política de utilização aceitável para uma instituição de ensino deve estabelecer as diretrizes e regras para o uso dos recursos tecnológicos disponíveis no ambiente escolar, garantindo a segurança, a privacidade e o bom uso desses recursos pela comunidade escolar (alunos, docentes e não docentes).

B. Objetivos

Os objetivos deste projeto passam por avaliar, numa primeira fase, a maturidade das instituições de ensino, mais concretamente os AE/ENA Portuguesas, e numa fase posterior pretende-se criar uma framework de recomendações e boas práticas tendo em conta os problemas que foram identificados no âmbito da cibersegurança.

Relativamente aos objetivos específicos, os mesmos são apresentados de seguida.

- 1 - Infraestrutura tecnológica
  Implementar sistemas de segurança na infraestrutura tecnológica para Identificar, Proteger, Detetar, Responder e Recuperar dos incidentes.

  1.1 - Ausência de planos de cópias de segurança

  Criar planos de cópias de segurança, consoante os vários equipamentos existentes nos Estabelecimentos de Ensino, para locais externos com elevados níveis de segurança, e com a cifragem dos dados na origem, aplicando algoritmos fortes para evitar a tentativa de acesso através da técnica de força bruta.

  1.2 - Infraestrutura ao nível da rede

  Apresentar algumas soluções, de código aberto, de sistemas de proteção como IDS(Intrusion Detection System) e/ou IPS (Intrusion Prevention System) para os AE/ENA passarem a gerir e a monitorizar as suas próprias comunicações, nos casos em que têm uma infraestrutura de acesso à internet própria. As instituições de ensino que têm apenas a infraestrutura da rede minedu, podem contratar outro provedor de serviço de internet porque têm autonomia para o fazer e assim melhoram a qualidade do serviço de internet.

  1.3 - Infraestrutura ao nível dos servidores

  Apresentar os principais cuidados que a equipa de TI deverá ter com os servidores existentes no AE/ENA, isto para garantir os mais altos níveis de segurança dos sistemas.
- 2 - Recursos humanos na área de cibersegurança
  Proteger a comunidade escolar, dotando-a de maiores conhecimentos na área da cibersegurança, é um ponto fulcral para garantir a segurança de todos. Está provado que a informação e formação eficaz reduz os riscos cibernéticos.
- 3 - Plano de Resposta a Incidentes
  Estabelecer um conjunto de procedimentos e orientações a serem seguidos em caso de ocorrência de um incidente de segurança, de forma que a equipa de segurança possa detetar, analisar, conter e mitigar o incidente de forma eficiente e eficaz. O plano tem como objetivo minimizar o impacto do incidente, reduzir o tempo de resposta e garantir a continuidade das operações críticas nos AE/ENA.
- 4 - Política de utilização aceitável (PUA)
  A política de utilização aceitável, difere de instituição para instituição, no entanto, existem algumas diretrizes e regras que podem ser comuns a todas as instituições

de ensino. Pretende-se apresentar uma PUA de exemplo que possa servir de base para as instituições de ensino utilizarem para garantir:
- A não utilização de conteúdo protegido por direitos autorais ou a disseminação de conteúdo ofensivo.
- Que os utilizadores são responsabilizados em caso de incumprimento, desta forma os utilizadores estão obrigados a seguir as regulamentações e leis aplicáveis, evitando potenciais ações legais e protegendo a instituição de ensino contra litígios.

II. Revisão da Literatura

O autor Frederico Manuel Ferreira Marques na dissertação de Mestrado [1], intitulada de ≪Estratégia integrada de avaliação e consciencialização cibernética em contexto escolar≫, do ano 2021, apresenta uma estratégia de consciencialização cibernética que foi implementada e avaliada em contexto escolar. O autor definiu três objetivos para o projeto e conseguiu concretizá-los. O primeiro objetivo era avaliar os comportamentos e atitudes dos alunos face à cibersegurança, para o efeito criou e disponibilizou um questionário a três turmas (finalistas) do 2º e 3º ciclo de escolaridade de uma instituição de ensino. O segundo objetivo era disponibilizar um segundo questionário para os utilizadores realizarem uma autoavaliação dos seus conhecimentos de cibersegurança, no final do questionário os utilizadores obtinham uma pontuação e um conjunto de recomendações. Para a elaboração dos dois questionários o autor recorreu à escala Likert. Por último, o terceiro objetivo do projeto era desenvolver um plano de aula, para abordar a curto-prazo, os temas da cibersegurança e ciberconsciência nas aulas de TIC e Educação para a Cidadania. Da análise realizada aos dados recolhidos através dos questionários, o autor conclui que existe um longo caminho a percorrer, sendo necessário sensibilizar a comunidade educativa sobre a necessidade de implementar estratégias de cibersegurança quer nas instituições de ensino, quer junto das famílias. Como trabalho futuro, o autor propõe que seja intensificada a promoção e divulgação de questionários de avaliação de atitudes e comportamentos noutros Estabelecimentos de Ensino para promover a segurança cibernética e os hábitos de ciberhigiene. Propõe também que os currículos das disciplinas de TIC e Cidadania passem a incluir um conjunto de aulas exclusivas sobre o tema Cibersegurança. Sugere também um planeamento de sessões autónomas de sensibilização destinadas aos docentes e não docentes com o intuito de melhorarem as suas habilidades de ciberconsciencialização, reduzindo os riscos de segurança cibernética.

Uma outra dissertação de Mestrado em Engenharia Informática que selecionei é da autoria de Bruno Pereira [2], intitulada de ≪Ciberexercícios na Comunidade Académica≫, do ano 2022, apresenta como projeto a preparação de um guião de como planear, executar e avaliar um ciberexercício no âmbito e contexto de uma instituição de ensino Superior. Embora o objetivo inicial da dissertação era cumprir com os objetivos propostos e normas planeadas pelo projeto CyberLab. O projeto CyberLab, tem como objetivo principal, a criação de um laboratório de inovação e experimentação de soluções de cibersegurança adaptadas aos diferentes contextos da Administração Pública. Contudo, com a ausência de recursos tecnológicos, o autor teve de reformular os objetivos da dissertação, que passou a ser a preparação do guião. O autor baseou-se nas normas e referências de segurança, nomeadamente, compilou 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. Concluída a fase de análise, o autor preparou dois exercícios, um sobre "Tabletop Ransomware (Lockbit)" e outro sobre "Red Team Vs Blue Team", nos quais descreve o objetivo do exercício, bem como apresenta uma proposta do planeamento e a avaliação a realizar. O autor recorreu a duas metodologias, o modelo CANVAS e análise SWOT para realizar o seu projeto. O autor comprovou da necessidade de investir em cibersegurança na Área de Ensino Superior em Portugal e, que os serviços administrativos das instituições de ensino necessitam de mais e melhor sensibilização para a temática e mais treino para conseguirem lidar com os vários tipos de incidentes. Constatou também que o processo de criar exercícios de cibersegurança envolve, para além do conhecimento técnico, é necessário envolver outras áreas como: logística, comunicação, e relações interinstitucionais. Como trabalho futuro, o autor propõe que o guião criado sirva de base para iniciar os desenvolvimentos dos ciberexercicios adaptados ao contexto das instituições de ensino superiores.

Foram analisados outros artigos de outros autores[3] [4] [5], mas com menor interesse para o presente tema.

III. Metodologia

Como metodologia irei adotar alguns métodos e técnicas nas várias etapas que descrevo de seguida.

- Escolha do Tema e Revisão da Literatura
  Optei por este tema por se tratar de um assunto emergente, preocupante e não consegui identificar trabalho já realizado para o público-alvo selecionado (AE/ENA). E para a revisão literária recorri a vários repositórios de instituições de ensino superior para consultar o trabalho já realizado.
- Elaboração do Questionário
  Para avaliar a maturidade de cibersegurança de alguns AE/ENA irei preparar um questionário cuidadosamente com questões abertas e fechadas que possam abranger os tópicos mais relevantes do tema em análise. Este questionário será disponibilizado online para um número restrito de 15 a 20 AE/ENA, a selecionar mais tarde e, direcionado aos Coordenadores TIC (Tecnologias da informação e Comunicação) e/ou Coordenadores PTE (Plano Tecnológico da Educação).
- Análise dos dados recolhidos
  A análise dos dados será objetiva e rigorosa e para o efeito os dados serão categorizados e analisados quantitativamente e qualitativamente.

- Preparação da framework de recomendações e boas práticas
  Por último, será criado o documento (framework) que será posteriormente disponibilizado aos AE/ENA que tiverem interesse em melhorar a segurança dos seus sistemas e dessa forma estarem mais bem preparados para enfrentar a nova realidade. Este documento (framework) terá a indicação dos Estabelecimentos de Ensino que contribuíram, bem como os dados estatísticos que resultaram da análise.

IV. Resultados Esperados

Como resultado esperado pretende-se que o framework de recomendações e boas práticas, os AE/ENA consigam adaptar a sua realidade aos desafios do cibercrime. Para cada um dos problemas/objetivos específicos identificados anteriormente, segue uma breve descrição do resultado esperado.

- 1 - Infraestrutura tecnológica
  Com uma melhoria constante da infraestrutura tecnológica, é esperado que os AE/ENA:
  - Protejam os seus dados, com a aplicação das melhores práticas de segurança da informação;
  - Reduzam o risco de novos incidentes, recorrendo a sistemas de análise de vulnerabilidades;
  - Cumpram os regulamentos e legislação em vigor;
  - Garantam confiança junto da comunidade escolar que a infraestrutura utilizada é segura.

  1.1 - Ausência de planos de cópias de segurança
  Com um plano de cópias de segurança, é esperado que os AE/ENA:
  - Garantam a segurança dos dados armazenados num determinado sistema, ao nível da confidencialidade, integridade e disponibilidade;
  - Garantam que as cópias de segurança que são realizadas periodicamente e sem falhas;
  - Garantam que é possível recuperar os dados, através de uma cópia de segurança, na eventualidade de um ciberataque ou até mesmo numa falha do equipamento/dispositivo, erro humano, entre outras razões que podem justificar o acesso à cópia de segurança.

  1.2 - Infraestrutura ao nível da rede
  Com a melhoria da infraestrutura de rede, é esperado que os AE/ENA:
  - Aumentem o desempenho, capacidade e a qualidade de transmissão de dados, garantindo assim um melhor serviço para a comunidade escolar;
  - Melhorem a segurança ao nível da rede, protegendo os dados confidenciais de terceiros;
  - Implementem sistemas de segurança como um IDS (Intrusion Detection System) e/ou IPS (Intrusion Prevention System), para analisarem o tráfego a circular na rede, para detetar e prevenir de novos incidentes.

  1.3 - Infraestrutura ao nível dos servidores
  Com a melhoria da infraestrutura ao nível dos servidores, é esperado que os AE/ENA:
  - Reforcem a segurança nos servidores, para evitar qualquer tipo de ciberataque (malware, phishing, engenharia social, entre outros);
  - Melhorem a segurança dos dados, com a implementação de ferramentas que ajudem e garantam a segurança dos dados armazenados nos servidores ou noutro tipo de equipamento como NAS (Network Attached Storage), reduzindo assim o risco de roubo de informação sensível;
  - Implementem ferramentas para analisar regularmente as vulnerabilidades existentes nos servidores;
  - Garantam que os serviços disponibilizados nos servidores estão atualizados. Que existem um controlo de acessos documentado. Que os serviços são acedidos apenas com ligações seguras, no caso concreto de um serviço Web, o acesso é realizado através do protocolo HTTPS (Hypertext Transfer Protocol Secure) e o certificado SSL (Secure Sockets Layer) é valido. O acesso externo apenas é realizado com recurso a uma VPN (Virtual Private Network).
- 2 - Recursos humanos na área de cibersegurança
  Com mais informação e formação sobre a cibersegurança, é esperado que os recursos humanos do AE/ENA:
  - Consigam compreender como podem surgir os ciberataques e quais são os sinais de alerta, desta forma passam a ter um papel mais responsável e vigilante na deteção e prevenção de ataques;
  - Consigam compreender as principais medidas de segurança e procedimentos adotar na resposta a incidentes em cibersegurança;
  - Sejam mais conscientes da importância da privacidade dos dados e entendam como protegê-la.
- 3 - Plano de Resposta a Incidentes
  Com o plano de resposta a incidentes, é esperado que os AE/ENA:
  - Consigam identificar rapidamente e conter os incidentes, minimizando o tempo de inatividade dos sistemas e os impactos que possam advir daí;
  - Consigam limitar os danos causados pelos incidentes, protegendo dados e sistemas críticos e prevenindo a propagação do incidente;
  - Consigam identificar o que originou o incidente e, desta forma, poderá ajudar a prevenir incidentes semelhantes no futuro;
  - Consigam responder rapidamente e eficazmente aos incidentes e, desta forma, a reputação da instituição de ensino não será afetada;
- 4 - Política de utilização aceitável (PUA)
  Com uma política de utilização aceitável, é esperado que os AE/ENA:
  - Melhorem a segurança da informação, diminuindo os riscos e aumentando a confiança na utilização dos recursos da tecnologia da informação;
  - Estabeleçam as orientações e limites éticos e legais para a utilização dos sistemas de informação e equipamentos da instituição de ensino;
  - Com a implementação da PUA possa ajudar a proteger

a instituição de ensino de riscos relacionados com a segurança da informação, como roubo de dados, perda de informações confidenciais, utilização indevida de recursos, entre outros;
- Promovam um ambiente de trabalho mais seguro e produtivo, onde os utentes/ex-utentes (alunos, docentes, não docentes e colaboradores) da instituição de ensino conhecem as regras e estão cientes das consequências caso violem a política.

V. Plano de Trabalho

A proposta de cronograma para desenvolver a tese, divide-se em 4 fases. Conforme quadro abaixo.

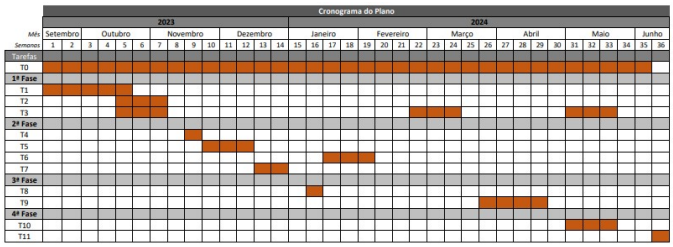

Figura 1. Cronograma do Plano

A redação da dissertação será realizada durante as 35 semanas (T0).

- A 1ª fase é composta por 3 tarefas. A primeira tarefa (T1) consiste na recolha bibliográfica e pesquisas do estado da arte. A segunda tarefa (T2) é para elaborar o índice do enquadramento teórico. Na última tarefa da primeira fase (T3) consiste na redação do enquadramento teórico.
- A 2ª fase é composta por 4 tarefas. A primeira tarefa (T4) consiste na preparação de um questionário para avaliar a maturidade de cibersegurança de algumas instituições de ensino. A segunda tarefa (T5) é para disponibilizar o questionário às instituições de ensino que foram selecionadas previamente. A terceira tarefa (T6), consiste na redação da primeira versão de uma possível framework de boas práticas de cibersegurana. Na última tarefa desta segunda fase (T7) pretende-se redigir a metodologia.
- A 3ª fase é composta por 2 tarefas. A primeira tarefa (T8) consiste em analisar, tratar e interpretar os dados recolhidos através do questionário. E para concluir esta terceira fase, a framework de boas práticas será ajustada de acordo com os resultados obtidos (T9).
- Por último, na 4ªfase do projeto, pretende-se concluir o documento final (T10) e por fim submetê-lo para posterior defesa (T11).

Referências

[1] Frederico Manuel Ferreira Marques. ≪Estratégia integrada de avaliação e consciencialização cibernética em contexto escolar≫. Em: *Instituto Politécnico de Leiria* (nov. de 2021), pp. 1–248.

[2] Bruno Daniel Monte Pereira. ≪Ciberexercícios na Comunidade Académica≫. Em: *Instituto Superior de Engenharia do Porto* (out. de 2022), pp. 1–94.

[3] Direção AE MemMartins. ≪Plano de Cibersegurança do AEMM≫. Em: *Agrupamento de Escolas MemMartins* (nov. de 2020), pp. 1–10.

[4] Joaquim Manuel Pires Santos. ≪Definição de política de segurança informatica no IPCB (Inst. Politécnico de Castelo Branco≫. Em: *Instituto Politécnico de Lisboa* (mar. de 2016), pp. 1–83.

[5] Rita Santos Gonçalves. ≪O fator humano da cibersegurança nas organizações≫. Em: *Universadade de Lisboa* (out. de 2019), pp. 1–52.