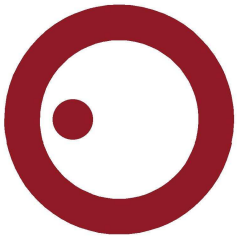


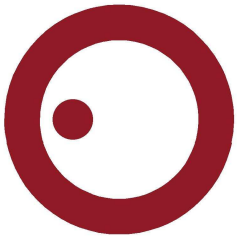
escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

ESTRATÉGIA INTEGRADA DE AVALIAÇÃO E CONSCIENCIALIZAÇÃO CIBERNÉTICA EM CONTEXTO ESCOLAR

FREDERICO MANUEL FERREIRA MARQUES

Leiria, Novembro de 2021



escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

ESTRATÉGIA INTEGRADA DE AVALIAÇÃO E CONSCIENCIALIZAÇÃO CIBERNÉTICA EM CONTEXTO ESCOLAR

FREDERICO MANUEL FERREIRA MARQUES
Número: 2190377

Projeto realizada sob orientação do Professor Doutor Mário João Gonçalves Antunes (mario.antunes@ipleiria.pt).

Leiria, Novembro de 2021

AGRADECIMENTOS

A concretização deste trabalho só foi possível graças à colaboração e suporte de um conjunto de pessoas a quem quero expressar os meus sinceros agradecimentos.

Ao Professor Mário Antunes docente da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, pela sua orientação, apoio, disponibilidade, saber transmitido e opiniões no esclarecimento de dúvidas e resolução de problemas.

À Professora Carina Silva docente da Escola Superior de Tecnologia da Saúde de Lisboa do Politécnico de Lisboa, pela sua colaboração no tratamento estatístico dos resultados, solução de problemas e esclarecimento de dúvidas.

Ao Professor Baltazar Rodrigues docente no mestrado em cibersegurança e informática forense no Instituto Politécnico de Leiria, pelos seus contributos com os comentários e sugestões de melhoria na adaptação dos questionários.

Ao Professor Carlos Rabadão docente do Instituto Politécnico de Leiria, pelos seus contributos com os comentários e sugestões de melhoria na adaptação dos questionários.

Ao Professor Lee Hadlington, psicólogo e Professor de ciberpsicologia na Nottingham Trent University, por autorizar a utilização dos questionários e pela sugestão de abordagem na adaptação das escalas.

À direção do Colégio Conciliar de Maria Imaculada (CCMI) por aceitarem participar no estudo autorizando a aplicação dos questionários aos seus alunos.

Deixo também um agradecimento ao Doutor Jorge Cotovio, pelo trabalho de revisão da dissertação.

Por fim, dirijo um agradecimento especial aos meus pais, pela sua coragem, apoio incondicional, incentivo e paciência no caminho para a concretização deste objetivo.

A eles dedico este trabalho!

RESUMO

A evolução tecnológica e a massificação do uso da Internet têm moldado a sociedade atual. O uso de dispositivos eletrónicos e da Internet e dos seus serviços, como a Web ou o e-mail, encontra-se, atualmente, massificado e tem uma abrangência global. Quer os cidadãos, quer as empresas, têm beneficiado imenso com o recurso às plataformas digitais, traduzindo-se numa fonte de criação de conhecimento, de incremento das relações interpessoais, de exploração de novas formas de entretenimento e de expansão da atividade social e económica.

As oportunidades que a Internet e os seus serviços oferecem, escondem alguns riscos emergentes e confinados à abrangência digital. É possível ver, cada vez mais, notícias associadas a ataques realizados na Internet, com recurso a formas cada vez mais sofisticadas. O cidadão comum é confrontado com vários tipos de ataques, normalmente, sob a forma de engenharia social, que se traduz em tentativas de extorsão, para obtenção de bens ou informação sobre a vítima. Relativamente às empresas, os desafios também são muitos, já que as motivações dos atacantes têm um largo espectro, variando desde a simples extorsão até à obtenção de informação sobre propriedade intelectual por parte das empresas concorrentes. A pandemia provocada pela COVID-19 acentuou ainda mais este problema, quer para os cidadãos, quer para as empresas e instituições, atendendo a que muitas pessoas foram forçadas a trabalhar, remotamente, e nem sempre com as condições técnicas e de segurança adequadas.

As escolas têm como missão a transferência de conhecimento e de competências reconhecidas pela sociedade, onde se incluem as competências digitais e a consciencialização para as questões relacionadas com a segurança no ciberespaço. A comunidade escolar é heterogénea e agrega vários perfis digitais, nomeadamente, os estudantes e os funcionários docentes e não docentes. Ao nível da consciencialização para as questões relacionadas com a cibersegurança, estes perfis estão igualmente em patamares diferentes, fruto do tipo de utilização, dos conhecimentos técnicos já adquiridos, bem como do nível socioeconómico a que pertencem.

Este relatório de projeto, apresenta-se uma estratégia integrada de consciencialização cibernética que foi implementada e avaliada em contexto escolar. Apresenta-se um estudo sobre as atitudes e comportamentos em relação à cibersegurança, em

meio escolar. Atendendo a que apenas é possível prevenir o que se consegue medir, o trabalho foi desenvolvido com recurso à medição dos comportamentos e das atitudes, através de dois questionários distintos, que utilizam uma escala de Likert. Foi igualmente disponibilizado e testado um autodiagnóstico, para medir as habilidades dos alunos em segurança cibernética, e um plano de aula de ciberconsciência, a aplicar nas unidades curriculares de TIC e/ou de Educação para a Cidadania. O trabalho teve como ponto de partida a utilização e adaptação de duas escalas já validadas, com aplicação em empresas e instituições na área da saúde. O interesse da comunidade científica e dos intervenientes (alunos, professores e funcionários) em analisar o nível de consciencialização para a cibersegurança, em meio escolar, constituiu a motivação para a realização deste trabalho.

Os resultados obtidos com a recolha dos questionários em três turmas do 6.º ano de escolaridade e ainda três turmas do 9.º ano, permitiram identificar comportamentos, tendências e más práticas relativamente às atividades realizadas online, quer em contexto escolar, quer em casa, em contexto de entretenimento. Numa segunda fase, procedeu-se ao desenvolvimento do questionário de autodiagnóstico, disponibilizado através de uma página web, que pretende avaliar o nível de cibersegurança e ciberconscientização na comunidade escolar, definindo um conjunto relativamente amplo de perguntas que se enquadram nos tipos de incidentes definidos na taxonomia de referência de incidentes de segurança e utilizada pela rede nacional de CSIRT. Na terceira fase, desenvolveu-se o plano de aula, para abordar os temas de cibersegurança e ciberconsciência, enriquecendo as atividades de ensino-aprendizagem das disciplinas de TIC e Educação para a Cidadania, em sala de aula.

A investigação decorreu no estabelecimento de ensino particular e cooperativo da cidade de Leiria, Colégio Conciliar de Maria Imaculada (CCMI). Além da caracterização da comunidade que participou no estudo e da análise dos resultados obtidos com os dois questionários, o trabalho de investigação englobou ainda dois elementos importantes que visam alertar para a consciencialização da cibersegurança no ambiente escolar: (i) a construção de um questionário de autoavaliação, sobre conceitos fundamentais de cibersegurança; (ii) o plano de uma aula, para abordar este tópico na disciplina de Tecnologias de Informação e Comunicação (TIC) e Educação para a Cidadania.

Globalmente, a medição efetuada e os resultados obtidos são promissores e permitem identificar as más práticas existentes, com vista a delinear um plano mais assertivo de consciencialização da cibersegurança. A metodologia de trabalho adotada, os questionários implementados e a aplicação de autodiagnóstico pode-

rão, facilmente, ser aplicados a outras instituições de ensino e a outros perfis da comunidade escolar, designadamente, aos docentes e pessoal não docente.

ABSTRACT

The technological evolution and the massive use of the Internet have shaped today's society. The use of electronic devices and of the Internet and its services, such as the web or the e-mail, is currently widespread and has a global reach. Both citizens and companies have benefited immensely from the use of digital platforms, turning it into a source of knowledge creation, a way of increasing interpersonal relationships, exploring new forms of entertainment and expanding social and economic activity.

The opportunities that the Internet and its services provide us with hide some emerging risks but also confined to digital coverage. It is possible to see more and more news associated with attacks carried out on the Internet using increasingly sophisticated methods. Ordinary citizens are faced with various types of attacks, usually in the form of social engineering, which translate into extortion attempts to obtain goods or information about the victim. As for the companies, the challenges are also many, as the attackers' motivations have a wide spectrum, ranging from simple extortion to obtaining information about intellectual property by competing companies. The pandemic caused by COVID-19 further accentuated this problem, both for citizens and for companies and for institutions, as many people were forced to work remotely and not always with the appropriate technical and security conditions.

The schools' mission is to transfer knowledge and skills recognized by society, which include digital skills and awareness of issues related to security in cyberspace. The school community is heterogeneous and includes several digital profiles, namely, of students and teaching and non-teaching staff. In terms of awareness of issues related to cybersecurity, these profiles are also at different levels, as a result of the type of use, the technical knowledge already acquired, as well as the socioeconomic level they belong to.

This report presents an integrated cyber awareness strategy that was implemented and assessed in school context. This dissertation presents a study on attitudes and behaviors in relation to cybersecurity in schools. Considering that it is only possible to prevent what can be measured, the work was developed by measuring behavior and attitudes, through two different questionnaires, using a Likert scale. It was also made available and tested a self-diagnosis to measure students' cybersecurity

skills and a cyberawareness lesson plan to be applied in the subjects of ICT and citizenship education disciplines.

The work had as its starting point the use and adaptation of two scales already validated, with application in companies and institutions that operate in the health services. The interest of the scientific community and stakeholders (students, teachers and staff) in analyzing the level of awareness of cybersecurity in schools was the motivation to carry out this work. The results obtained with the through the application of questionnaires in three 6^{th} grade classes and three 9^{th} grade classes, allowed for the identification of behaviors, trends and bad practices while developing activities online, either in the school context or at home, while engaging in entertainment activities.

In a second phase, the web self-diagnosis questionnaire was developed and made available through a web page, which aims at assessing the level of cybersecurity and cyberawareness in the school community, defining a relatively broad set of questions that fit the type of incident defined in the reference taxonomy of security incidents and used by the national CSIRT network.

In the third phase, a lesson plan was developed to address the issues of cybersecurity and cyberconsciousness to enrich the teaching-learning activities of the subjects of ICT and Education for Citizenship in the classroom.

The research took place in a private and cooperative teaching establishment in the city of Leiria, namely the Colégio Conciliar de Maria Imaculada (CCMI). In addition to the characterization of the community that participated in the study and the analysis of the results obtained with the two questionnaires, the research work also encompassed/gathered as a whole two important elements that aimed at raising awareness of cybersecurity in the school environment: i) the development of a self-assessment questionnaire on fundamental cybersecurity concepts; ii) the lesson plan to address this topic in the subject of Information and Communication Technologies (ICT) and citizenship education disciplines.

Overall, the measurement carried out and the results obtained are promising and allow for the identification of the existing bad practices, in order to outline a more assertive plan to raise cybersecurity awareness. The work methodology adopted, the questionnaires implemented and the self-diagnosis could easily be applied to other educational institutions and to other profiles of the school community, namely, teachers and non-teaching staff.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ABIS	Abbreviated impulsiveness scale.
ATC-IB	Attitudes towards cybersecurity and cybercrime in business.
BYOD	Bring Your Own Device.
CCMI	Colégio Conciliar de Maria Imaculada.
CIA	Confidentiality, Integrity e Availability.
COVID-19	Corona Virus Disease 2019.
CSA-S	Cybersecurity Attitudes In Schools.
CSB-S	Cybersecurity Behaviors In Schools.
CSIRT	Computer Security Incident Response Team.
DGEEC	Direção-Geral de Estatísticas de Educação e Ciência.
ENISA	European Union Agency for Cybersecurity.
HAIS-Q	Human Aspects of Information Security Questionnaire.
IBM SPSS	Statistical Package for the Social Sciences.
ISA	Information Security Awareness.
ISO	International Standardization Organization.
ISP	Internet Service Provider.
KAB	knowledge, attitude and behavior model.

MENA	Middle East and North Africa region.
NATO	North Atlantic Treaty Organization.
OCS	Online Cognition Scale.
ODS	Objetivos de Desenvolvimento Sustentável.
OIG	Organização Inter Governamental.
ONG	Organização Não Governamental.
OTAN	Organização do Tratado do Atlântico Norte.
PME	Pequenas e Médias Empresas.
RGPD	Regulamento Geral de Proteção de Dados.
RScB	Risky cybersecurity behaviours scale.
TI	Tecnologia da Informação.
TIC	Tecnologias de Informação e Comunicação.
UE	União Europeia.
WWW	World Wide Web.

1

INTRODUÇÃO

A Internet, parte integrante do ciberespaço, é constituída por uma complexa infraestrutura tecnológica, onde se podem encontrar vários componentes essenciais para a comunicação digital à escala global. A evolução tecnológica da Internet, especialmente ao longo das últimas duas décadas, a sua globalização e o acesso universal para todos os indivíduos e empresas, alterou significativamente a forma como comunicamos e interagimos em sociedade (Kohn e Moraes, 2007). O aparecimento do serviço *World Wide Web (WWW)* e a partilha e acesso fácil e de forma distribuída, à informação facilitaram sobremaneira, o dia-a-dia das pessoas, mas também expuseram algumas fragilidades no relacionamento daquelas com a tecnologia. Outros serviços tiveram, igualmente, um impacto positivo nas pessoas e nas empresas, como é o caso do correio eletrónico (e-mail) e a transferência remota de ficheiros.

Da mesma forma, as mensagens instantâneas, as chamadas, videoconferências, e as redes sociais, encurtaram distâncias e revolucionaram a comunicação, permitindo alcançar e manter ligações sociais, que, de outra forma, não seriam possíveis. A Internet revolucionou também a área do entretenimento, com a multiplicação das plataformas de *streaming* e jogos online, onde os utilizadores escolhem o que pretendem ver ou jogar, a partir de qualquer lugar. Por outro lado, tornou possível a compra de quase tudo o que se quiser, a partir de casa, e revolucionou a aprendizagem, aproveitando a curiosidade natural das crianças e os recursos disponíveis online (Capobianco, 2010).

É, hoje, inegável a ligação entre a tecnologia e a forma de vida em sociedade, com a dependência dos serviços da Internet, quer a nível pessoal, quer em contexto empresarial. De uma forma geral, os utilizadores da Internet sãp obrigados a passar mais tempo online, quer em atividades de entretenimento, quer no desempenho da atividade profissional (Kemp, 2020). Na verdade, a pandemia provocada pelo COVID-19 é um bom e recente exemplo, onde a dependência dos serviços da Internet e o tempo dispendido online aumentaram, quer para entretenimento, quer no âmbito da atividade profissional. A necessidade de distanciamento social levou a um recurso massivo ao teletrabalho e as atividades letivas de todos os níveis de ensino foram

igualmente transferidas para plataformas de streaming, como o Zoom , Google Meet ou o Microsoft Teams (Singh et al., 2020). De acordo com (Smahel et al., 2020), antes da pandemia provocada pelo COVID-19, as crianças e os jovens europeus, com idades entre os 9 a 16 anos, usavam a Internet, em média, durante 167 minutos por dia. Em todos os exemplos de teletrabalho é possível evidenciar o necessário aumento da exposição de informação confidencial, transportada em canais desprotegidos, em larga medida devido à necessidade, muitas vezes de forma consentida, de ter acesso a informação privilegiada ou simplesmente para fazer parte de um grupo ou rede social online (Leidner, 2020; República, 2020).

O crescente aumento do número de utilizadores ligados online na Internet não tem parado de aumentar(KEMP, 2021; Portugal, 2020). A expansão da Internet à escala global e a sua heterogeneidade têm revelado várias fragilidades ao nível da utilização legítima e legal. Tomem-se como exemplos a divulgação e acesso fácil a conteúdos protegidos por direitos de autor, a difusão massiva de e-mails com informação não solicitada pelos utilizadores (por exemplo, os e-mails de SPAM), ou ainda a divulgação de discursos de ódio, o *defacing* e o rapto digital (6dg.co.uk, 2021; Cibersegurança Portugal, 2021). Estes exemplos estão associados a atividades criminosas que são efetuadas no ciberespaço e que têm como objetivo principal provocar danos (físicos ou materiais) nas vítimas (ENISA, 2020; Europol, 2020).

Os ciberataques têm aumentado e têm-se tornado mais anonimizados e sofisticados. O espectro de atividades criminosas é vasto, bem como o seu grau de severidade e impacto nos computadores ou pessoas afetadas (Cibersegurança Portugal, 2021). Para fazer face aos ataques que vão sendo conhecidos, são normalmente implementadas e desenvolvidas soluções tecnológicas para proteger a infraestrutura de rede e de servidores de possíveis ameaças que possam ser endereçadas aos computadores e aplicações. A implementação de sistemas de deteção de intrusões, *firewalls* e programas para detetar vírus, são alguns exemplos de soluções tecnológicas que poderão proteger e, em certos casos, reagir a ações maliciosas que possam ser iniciadas por um atacante a uma infraestrutura de rede (Canongia e Mandarino Junior, 2010).

Embora estas soluções protejam, detetem e, em certos casos, reajam a cenários de ameaça e ataque iminente, para alguns tipos de ataques a melhor estratégia assenta na prevenção, nomeadamente na consciencialização dos utilizadores (Zwilling, Klien et al., 2020). A educação dos utilizadores para a correta identificação de um e-mail de *phishing* e para os comportamentos corretos a adotar são um dos vários exemplos que podem ser elencados. A adoção, a montante, de comportamentos responsáveis na utilização da Internet poderá minimizar a ocorrência de ameaças e ataques a

jusante, que coloquem em risco a disponibilidade da infraestrutura de rede e dos seus serviços.

E mesmo com a adoção de medidas de cibersegurança consideradas suficientes, os utilizadores continuam a ser o elo mais fraco na cibersegurança, estando diretamente relacionados com perdas financeiras, violações de dados e múltiplos incidentes de segurança (Sabillon et al., 2019). Isto acontece porque os utilizadores têm de tomar regularmente decisões de segurança cruciais, que podem comprometer a segurança da informação, sendo a sensibilização considerada essencial para o desenvolvimento destas capacidades (Mouton et al., 2014), pois ajudará os utilizadores a compreender os riscos do uso da Internet, a importância de proteger as informações pessoais e as consequências dos comportamentos incorretos (Kritzinger e Solms, 2010).

Considerando a atual realidade social, onde há cada vez mais pessoas a passar mais tempo online e se verifica um crescimento em número e sofisticação dos ataques efetuados no ciberespaço (Zwilling, Klien et al., 2020), torna-se ainda mais evidente a necessidade de desenvolvimento de competências de cibersegurança dos utilizadores, como forma de fazer face aos perigos (Richardson et al., 2020). No caso particular das escolas, com a massificação do ensino, passou-se de um modelo de educação essencialmente elitista e homogéneo, para um ambiente globalizado e heterogéneo, que assenta no princípio da inclusão e equidade para que todos tenham as mesmas oportunidades (I.Arends, 2008).

As escolas, enquanto locais de diversidade cultural, étnica, económica e social, requerem a adaptação dos seus processos para atingir os seus objetivos fundamentais: ensinar e preparar os alunos para serem cidadãos ativos e conscientes (I.Arends, 2008). Uma das grandes alterações para fazer face a esta realidade, foi a evolução digital, que permitiu modernizar os processos de gestão e educação. Na aprendizagem, esta transformação assume várias dimensões: a disponibilização de equipamento individual, acesso de qualidade à Internet a partir das instalações da escola, acesso a recursos educativos digitais e a ferramentas de colaboração em ambientes digitais, e ainda a capacitação de docentes através da aquisição de competências necessárias para aplicação em contexto digital. Relativamente à modernização dos processos de gestão, as escolas passaram a dispor de um conjunto de métodos que lhes permite recolher e armazenar os dados pessoais de alunos e funcionários. Desta forma, aumentaram a sua dependência da infraestrutura tecnológica de suporte à gestão escolar, como sejam as avaliações e os processos dos alunos, entre outros exemplos (Conselho de Ministros n.º 137/2007, 2007).

No entanto, o aumento da dependência das escolas, dos serviços digitais e da Internet, bem como o uso frequente de computadores e dispositivos móveis, têm conduzido a uma maior exposição dos utitilizadores a vulnerabilidades, tal como acontece em outras instituições, como as empresas. Embora a utilização de tecnologia específica contribua para a proteção das instituições, dos utilizadores, dos seus dados e um cumprimento das imposições legais, a consciencialização dos utilizadores desempenha um papel muito importante na prevenção de incidentes de cibersegurança. Assim, os utilizadores em contexto escolar (alunos, docentes e pessoal não docente) têm de desenvolver competências que lhes dêem garantias de um uso eficiente e protegido do ciberespaço, com vista à prevenção de incidentes de cibersegurança e evitando potenciais efeitos negativos nos equipamentos que utilizam (Chen e Shen, 2019; Peker et al., 2018).

Estes conhecimentos podem ser adquiridos por formação pessoal ou nas organizações, como parte de um plano que procura assegurar algum nível de segurança e operacionalidade, pela implementação de planos de cibersegurança, que salvaguardem a dimensão técnica, da política organizacional, legal, económica e a do comportamento humano (Cibersegurança Portugal, 2019). As escolas, pela sua função, têm a responsabilidade de salvaguardar os seus sistemas de informação e os dados, disponibilizar um acesso seguro às tecnologias digitais como parte da experiência de ensino e aprendizagem, mas também preparar os alunos para fazer face à problemática da cibersegurança. Considerando que os alunos têm diferentes níveis de conhecimento informático e diferentes níveis de ciberconsciencialização, a escola enfrenta um grande desafio na tarefa de ciberconsciencialização e educação.

1.1 RELEVÂNCIA DO ESTUDO

O fator humano é de extrema importância na cibersegurança, tornando-se evidente que o uso de tecnologias de segurança não é por si só suficiente para garantir a proteção dos utilizadores e dos equipamentos, aquando da existência de um ciberataque (proofpoint.com, 2019; Richardson et al., 2020). Os utilizadores são assim considerados o elo mais fraco, no que à cibersegurança diz respeito (Mittal, 2015), sendo por isso a primeira linha de defesa que deve ser considerada numa estratégia de cibersegurança. São vários os documentos que dão corpo à necessidade de aumentar o nível de ciberconsciencialização, como o relatório produzido pelo Centro Nacional de Cibersegurança (CNCS), com os indicadores sobre as atitudes, comportamentos, educação e sensibilização, em relação à cibersegurança dos indivíduos e organizações

em Portugal (Cibersegurança Portugal, 2020). A edição mais recente desde relatório (dezembro de 2020) conclui que o nível de atitudes e comportamentos apresentados não são suficientemente adequados para fazer face às ciberameaças e, embora apresentem uma preocupaão especial com as ameaças de phishing e software malicioso, não apresentam comportamentos preventivos adequados. Conclui ainda o mesmo relatório que os valores apresentados em Portugal estão abaixo da média da UE em muitos indicadores, destacando a necessidade de realizar um esforço acrescido de educação e sensibilização para as atitudes e os comportamentos mais adequados em cibersegurança (Cibersegurança Portugal, 2020).

A escola pode contribuir para a construção da educação para a cibersegurança, desenvolvendo práticas de segurança de informação e trabalho de consciencialização, que permitam aos alunos tirar o máximo partido das tecnologias, e tomar decisões informadas, conscientes e coerentes. Para tal, necessita de saber como agir com base no perfil dos seus alunos e, reconhecendo a sua diversidade, encontrar formas de lidar com as diferenças, adequando os processos de aprendizagem às caraterísticas e condições dos alunos. A motivação para a realização deste trabalho é no sentido de caracterizar uma população de estudantes e identificar o seu perfil para as questões relacionadas com os comportamentos e atitudes dos estudantes nas questões relacionadas com cibersegurança. Com base na caracterização efetuada, as escolas passam a dispor de uma ferramenta de gestão que permitirá definir estratégias de ensino-aprendizagem, onde sejam trabalhadas as questões relacionadas com educação para a (ciber)cidadania, ciberconsciencialização e aspetos técnicos relacionados com a tecnologia informática.

1.2 CONTEXTO ESCOLAR

O trabalho apresentado neste relatório de projeto foi desenvolvido no Colégio Conciliar de Maria Imaculada, localizado em Leiria. Trata-se de um estabelecimento de ensino de referência, com uma larga história que começa em 1941, com o nascimento da Comunidade da Casa da Cruz da Areia, designando-se na altura, "Colégio Missionário de Nossa Senhora de Fátima", destinando-se a alunas internas, a frequentar o Ensino Primário. Mais tarde, no ano letivo de 1964/1965, alarga a sua oferta ao 2º Ciclo, e numa terceira fase, após a ampliação das instalações até ao 3º ciclo. A partir de 1969, passa a designar-se "Colégio Conciliar de Maria Imaculada", sendo em 1975, fruto da revolução de abril de 1974, transformado numa cooperativa de ensino, designada de "Cooperativa de Ensino e Cultura da

Cruz d'Areia (CECCA)", funcionando como cooperativa de Irmãs-religiosas, Pais e Professores. Em 1981, após a publicação do Dec. Lei n° 553/80, voltou ao modelo de funcionamento anterior, encontrando-se desde o ano lectivo 1995/96 em regime de Contrato de Associação com o Ministério da Educação para os 2º e 3º ciclos, recebendo alunos da sua área de abrangência (Leiria), como definido pelo Ministério da Educação.

Este estudo, contou com a participação de três turmas de alunos de 6.º ano e outras tantas do 9.º, num total de cerca de 164 alunos, com idades compreendidas entre os 11 e 15 anos. Cada um destes estudantes respondeu a dois questionários distintos, um para os comportamentos e outro para as atitudes. A recolha e armazenamento de dados foi realizada através do preenchimento dos questionários disponibilizados na plataforma LimeSurvey (https://www.limesurvey.org/) onde, em cada pergunta, é avaliado o grau de concordância dos inquiridos, através de uma escala de Likert. Esta tarefa teve lugar durante o mês de abril de 2021, numa aula presencial da disciplina de TIC. A aula iniciou-se com a apresentação dos objetivos dos questionários, sendo de seguida realizada a recolha de respostas, tal como consta no plano no anexo C.1.

1.3 OBJETIVOS

A utilização da Internet e de equipamentos digitais vai continuar a fazer parte da realidade dos alunos em contexto escolar. Nesse sentido, o investimento que possa ser realizado na formação de alunos e docentes em cibersegurança, designadamente na definição de estratégias de consciencialização, é um passo em frente na utilização eficiente, racional e segura da Internet. Para uma correta e assertiva acção da escola na definição de estratégias de formação, é fundamental caracterizar a comunidade escolar sobre os conhecimentos gerais de cibersegurança, bem como sobre os comportamentos e atitudes adotados pelos seus alunos e docentes.

Face ao enquadramento exposto anteriormente, três questões de investigação guiaram o trabalho e a investigação realizada, designadamente:

1. *Com os questionários CsA-S e CsB-S*

   Globalmente, para os alunos dos 6.º e 9.º anos, que correspondem à conclusão dos 2º e 3º ciclos de ensino, qual o nível de comprometimento existente para os comportamentos e atitudes em cibersegurança?

2. *Com a disponibilização dos questionários de autodiagnóstico*

É possível, reforçar e melhorar, de forma autónoma, as competências de cibersegurança?

3. *Qual o impacto da definição de um plano de aula*

   Qual o impacto da definição de um plano de aula para os aspetos relacionados com a cibersegurança, na disciplina de Educação para a Cidadania ou TIC?

No âmbito deste projeto, foram definidos e concretizados com sucesso, os seguintes objetivos:

1. Avaliar os comportamentos e atitudes dos alunos face à cibersegurança, e assim preparar de uma forma mais adequada as estratégias de ensino-aprendizagem, formação e consciencialização. Para tal, foram disponibilizados dois questionários de medição dos comportamentos e das atitudes em contexto escolar, segundo uma escala de Likert. Foi efetuada uma análise dos dados recolhidos e dos elementos de caraterização da população (aspetos sociodemográficos: idade, género, nível de ensino e grau académico dos pais), com o intuito de identificar padrões que possibilitem a criação de conteúdos e estratégias de educação e sensibilização em matéria de cibersegurança. As escalas utilizadas correspondem a adaptações de outras já existentes, aplicadas em domínios diferentes, como é o caso de empresas ou instituições de saúde.
2. Disponibilizar um questionário de auto-avaliação dos conhecimentos de cibersegurança. O questionário tem perguntas que se enquadram nas áreas de classificação de incidentes da Rede Nacional de CSIRT definidas pelo CNCS e é direcionado principalmente aos alunos e docentes. Pretende-se que os utilizadores façam uma auto-avaliação dos seus conhecimentos, obtendo no final uma pontuação e uma lista de recomendações para leituras futuras, tendo em conta as respostas dadas às perguntas.
3. Desenvolver um plano de aula que possa ser aplicado em disciplinas onde a ciberconsciencialização seja um tópico abordado. Nesse sentido, o plano de aula apresentado refere-se a um bloco de 90 minutos e está preparado para ser lecionado nas disciplinas de Educação para a Cidadania e/ou TIC. O desenvolvimento deste plano de aula é de enorme importância, já que permite envolver a comunidade educativa e não apenas os docentes das disciplinas tecnológicas. O objetivo é de, a curto-médio prazo, as questões relacionadas com a cibersegurança fazerem parte do plano de trabalhos de disciplinas com menor cariz tecnológico e passarem a ser tratadas como questões de cidadania.

1.4 ESTRUTURA DO DOCUMENTO

Este relatório de projeto está organizado em 5 capítulos: (capítulo 1) Introdução, (capítulo 2) Revisão de literatura, (capítulo 3) Desenvolvimento, (capítulo 4) Análise de resultados e (capítulo 5) Conclusões.

O capítulo 1 inicia-se com um contextualização da realidade social atual, a relevância do estudo em causa, o seu contexto de realização e os objetivos deste projeto. É também aqui que se encontra a descrição da estrutura do documento.

No capítulo 2, são apresentados os conceitos fundamentais no contexto da cibersegurança e de "Cidadania Digital", assim como os resumos de alguns trabalhos e artigos científicos publicados nas seguintes áreas: problemática da compreensão e consciencialização dos riscos de cibersegurança; influência do fator humano na cibersegurança; impacto da consciencialização dos utilizadores na cibersegurança e sobre o planeamento de cibersegurança em escolas e organizações. Apresenta também um breve sumário sobre a dinâmica do comportamento dos utilizadores e a sua variação no espaço e no tempo.

O capítulo 3 apresenta seis secções. Na secção 3.1 é abordada a metodologia adotada na construção das novas escalas de CsB-S (Cybersecurity Behaviors In Schools) e CsA-S (Cybersecurity Attitudes In Schools), as desisões envolvidas na construção do questionário de Auto-diagnótico e do plano aula. É também neste capítulo que se apresenta o resultado do trabalho realizado, designadamente a nova escala de atitude (secção 3.2), a nova escala de comportamentos (secção 3.3), o questionário de autodiagnostico (secção 3.5) e o plano de aula (secção 3.4). A secção 3.4 apresenta informação sobre os planos de aula, as motivações associadas às decisões tomadas e o trabalho resultante. Da mesma forma, a secção 3.5 apresenta as motivações e decisões tomadas na construção do questionário de Auto-diagnóstico e o resultado obtido. A concluir este capitulo, temos a secção 3.6, que apresenta o resumo do trabalho realizado, enquadrando-o com os objectivos deste trabalho.

O capítulo 4 apresenta uma caracterização do publico de aplicação dos questionários (secção 4.1), uma análise por item/pergunta dos resultados recolhidos na escala de atitudes (secção 4.2) e comportamentos (secção 4.3) e a análise efetuada para responder às perguntas da investigação (secção 4.4).

Finalmente, no capítulo 5 são apresentadas as conclusões, o trabalho futuro e as limitações identificadas.

2

REVISÃO DA LITERATURA

Este capítulo inicia-se com a sintetização, na Secção 2.1 dos principais conceitos necessários para a leitura e compreensão do documento. De seguida, na secção 2.2, são apresentados os principais trabalhos relacionados com a ciberconsciencialização, designadamente em contexto escolar, empresarial e outros.

2.1 CONCEITOS FUNDAMENTAIS

Os indivíduos dependem das TIC na sua vida quotidiana, resultado de uma quase omnipresente adoção de tecnologia. No entanto, o constante desenvolvimento de novas ameaças torna extremamente importante a adoção de medidas de proteção.

Neste contexto, a cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção, que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem (Conselho de Ministros, 2019).

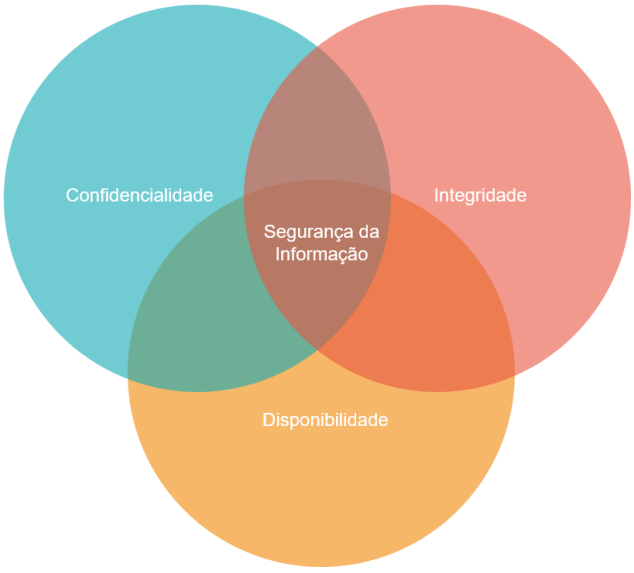


Figura 1: Segurança da informação com base na triade CIA

Tendo em conta a definição de cibersegurança da Resolução do Conselho de Ministros n.º 92/2019, importa apresentar os significados de alguns termos utilizados. Assim, a confidencialidade traduz a ideia de evitar uma aquisição não autorizada da informação (Caldas e Freire, 2013). A integridade da informação procura garantir que a informação seja verdadeira e permanece inalterada (Caldas e Freire, 2013). O ataque à disponibilidade de computadores ou recursos da informação traduz-se na privação dos utilizadores autorizados em aceder aos sistemas para o desempenho das suas tarefas (Caldas e Freire, 2013).

O não repúdio refere-se à garantia de que uma entidade não pode negar a autoria da informação.

No entanto, hoje sabe-se que uma segurança eficaz e que perdura, não se baseia apenas em soluções tecnológicas, mas também no nível de consciencialização para a cibersegurança e dos comportamentos dos indivíduos na utilização dos sistemas. Neste contexto, importa definir o que se entende por consciencialização em cibersegurança e cidadania digital. De acordo com Kilic e Karakuş (2021), consciencialização em cibersegurança (*digital awareness*) é a consciência dos conhecimentos, habilidades e atitudes necessários para que os indivíduos utilizem as ferramentas digitais de forma eficaz.

Segundo Zook (2019), cidadania digital refere-se ao uso responsável da tecnologia por qualquer pessoa que use computadores, a Internet e dispositivos digitais para se envolver com a sociedade em qualquer nível.

O termo ciber-higiene é também importante e está associado à adoção de práticas que visam reduzir as vulnerabilidades das TIC podendo definir-se como as "*(. . .) práticas fundamentais geralmente necessárias para estabelecer e manter a segurança de qualquer sistema de TI*" (Barbas e Sancho Hirane, 2018).

2.2 PUBLICAÇÕES RELACIONADAS

Este trabalho pretende conhecer os comportamentos e atitudes em relação à cibersegurança dos alunos que frequentam os estabelecimentos de ensino e dotar as instituições de meios que permitam identificar e combater os problemas. Pretende-se assim contribuir para a construção da consciencialização social necessária para fazer face aos riscos de estar online.

Uma pesquisa prévia permitiu identificar vários trabalhos que pretendem contribuir para uma melhor cibersegurança, abordando concretamente a problemática da consciencialização dos utilizadores.

2.2.1 *Ciberconsciencialização nas escolas*

O estudo realizado por Slusky e Partow-Navid (2012) denominado *«Students information security practices and awareness»* apresenta os resultados de um inquérito realizado entre os alunos do College of Business and Economics da California State University, em Los Angeles, no ano de 2011, com o objetivo de avaliar os conhecimentos e as habilidades básicas de Segurança da Informação. O estudo foi realizado com base nas respostas a um questionário composto por 29 perguntas organizadas nas categorias habilidades informáticas, práticas e consciencialização, com o intuito de obter/identificar dados demográficos, recursos e habilidades de TI, riscos e contramedidas dos alunos participantes. O estudo documenta as descobertas e revela várias caraterísticas das práticas e consciencialização dos intervenientes no questionário, das práticas dos alunos, da sua consciência do risco e habilidades informáticas, computação móvel, criptografia de dados, redes sociais e correlação entre prática e consicencialização documentados neste trabalho. O estudo aponta como principal problema da consciencialização para a cibersegurança, a forma como os alunos aplicam esse conhecimento em situações do mundo real, e não a falta de conhecimento de segurança.

O artigo de Livingstone et al. (2011), denominado *«Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries»* do ano de 2011, aplicou um questionário em vinte cinco países Europeus, em ambiente escolar. Foi aplicado a um conjunto de crianças e jovens com idades compreendidas entre 9 e 16 anos, procurando contribuir para o conhecimento das experiências e práticas online das crianças e pais europeus em relação ao uso da Internet e novas tecnologias e, desta forma, promover a consciencialização e promoção, nos vários países envolvidos e internacionalmente, de um ambiente online mais seguro.

Entre as descobertas apontadas destacam-se:

- a maioria das crianças que usam a Internet acede a partir de casa, o que sugere que, na maioria dos casos os pais estão mais bem posicionados para mediar o uso da Internet de seus filhos.

- os adolescentes estão online a partir de casa, principalmente nos seus quartos, o que representa um desafio para os pais.
- A escola é o segundo local seguro onde as crianças normalmente utilizam a Internet, dando aos professores um papel importante na educação sobre o uso seguro e responsável da Internet.
- Embora o computador pessoal seja o meio mais comum de acesso à Internet, em média as crianças utilizam dois dispositivos para estarem online.
- Os adolescentes ficam cada vez mais tempo online (o que levanta a questão do uso excessivo), e as crianças começam a estar online cada vez mais precocemente.

Assim, Livingstone et al. (2011), aponta como prioritária uma intervenção que melhore a consciência parental e que se foque nos utilizadores mais jovens, com um suporte da indústria a fornecer o máximo de segurança e privacidade por omissão, para as crianças que usam os seus serviços. Adicionalmente, considera também essencial melhorar a cidadania digital nas crianças e jovens, encorajando as crianças a serem responsáveis pela sua própria segurança, em vez de dependerem de restrições, e garantindo maior disponibilidade de conteúdos positivos apropriado para as suas idades.

O artigo *«Impact of users security awareness on desktop security behavior: A protection motivation theory perspective»*, realizado no College of Business, da University of North Texas em 2016 por Hanus e Wu (2016), utiliza a teoria da motivação para estudar o impacto nos comportamentos de segurança e ciberconsciencialização. Os autores examinam os papéis desempenhados pela consciência nos processos cognitivos e apresentam resultados que indiciam que a consciencialização de segurança afeta significativamente a perceção de gravidade, eficácia da resposta, autoeficácia e custo da resposta. Neste estudo, Hanus e Wu (2016) dão uma perceção aprofundada sobre a consciencialização da segurança da informação dos utilizadores domésticos, investigando este fenómeno com base na teoria da motivação de proteção, acrescentando ao conhecimento atual a consciência de segurança como um antecedente de comportamentos de proteção. Enfatiza, assim, a natureza multidimensional da consciência de segurança e a necessidade de promoção das melhores práticas de consciencialização que tenham em conta a natureza complexa dos indivíduos para a segurança da informação entre os utilizadores domésticos.

O artigo designado de *«A survey on Internet usage and cybersecurity awareness in students»* de Tirumala et al. (2016) foi publicado em 2016, e apresenta os resultados de uma pesquisa sobre o uso de Internet e ciberconsciencialização em três

grupos de alunos com idades compreendidas entre 8 e 21 anos da Nova Zelândia. A recolha de dados foi realizada com recurso a um questionário com respostas validades de 2214 participantes. Os resultados obtidos permitiram concluir que, à data da sua realização, os alunos com idades entre 8 e 12 anos tinham um nível de ciberconsciencialização baixo. É igualmente possível concluir que os alunos não estavam familiarizados com os termos de cibersegurança, nem tinham conhecimentos das ferramentas de segurança para proteger computadores, tablets e smartfones utilizados nas escolas ao abrigo da política BYOD. Por outro lado, o uso da Internet está a aumentar diariamente, em todas as faixas etárias e existe alguma consciência dos aspetos básicos ou fundamentais da cibersegurança. Concluindo que o trabalho de consciencialização em cibersegurança é necessário, e sugerindo-se a criação de programas de ciberconciencialização para estudantes.

O trabalho de Zwilling, Lesjak et al. (2019), denominado *«How to deal with the awareness of cyber hazards and security in (Higher) education»* foi publicado em 2019 e aborda a problemática do uso da Internet e os seus perigos, procurando determinar o nível de consciencialização e comportamento de segurança dos alunos do ensino superior. O objetivo é aumentar o nível de ciberconsciencialização e preparar os alunos para viver e trabalhar online de forma mais segura, fornecendo soluções teóricas e práticas relacionadas com a cibersegurança, que podem ser utilizadas em vários grupos de utilizadores, desde crianças do ensino básico e secundário, a empregados e reformados. Para atingir este objetivo, foi distribuído um mini questionário em papel aos alunos de licenciatura e mestrado da International School for Social and Business Studies, com perguntas para testar a familiaridade com a cibersegurança em geral e o nível de ciberconsciencialização aos riscos a que estão expostos online. Os resultados apontam para a necessidade e espaço para melhorias no que diz respeito à ciberconsciencialização que o ensino pode e deve fornecer.

O trabalho *«Planning for Cyber Security in Schools: The Human Factor.»* efetuado na área da cibersegurança nas escolas por Richardson et al. (2020), foi realizado na *Columbus State University* nos Estados Unidos e publicado em 2020. Analisa a problemática da cibersegurança nas escolas, procurando identificar os problemas, os riscos a que estão expostas e os motivos que as tornam alvos atrativos para os cibercriminosos. Aborda, também, a problemática do fator humano e a forma como os alunos podem influenciar a segurança. O estudo observa a existência de grandes e contínuos avanços na tecnologia, mas sem o respetivo acompanhamento no lado humano. O estudo conclui que a ciberconsciencialização é essencial para mitigar as vulnerabilidades relacionadas com o fator humano e sugere que uma abordagem única (*onesize-fits-all*) escolar na mitigação de riscos de cibersegurança não está

a funcionar, considerando necessário mais trabalho de mitigação de ameaças dos utilizadores, para o sucesso a longo prazo da cibersegurança escolar.

O artigo *«Oliver Wyman Forum Global Cyber Risk Literacy and Education Index»* de Mee et al. (2020), publicado em outubro de 2020, procura medir o nível de compreensão e consciencialização dos riscos de cibersegurança, com base em cinco fatores chave, considerados necessários para o desenvolvimento da literacia digital. Inclui um conjunto alargado de países e procede à sua classificação por nível de literacia, considerando como fatores chave, a motivação pública para tomar medidas de proteção, as politicas governamentais para o melhoramento da compreensão da problemática da cibersegurança, o foco dos estabelecimentos de ensino em melhorar a literacia digital da população, o mercado de trabalho, a forma como os empregados procuram aprofundar a sua ciberconsciencialização e o acesso equitativo à informação sobre ameaças no ciberespaço no sistema educativo formal ou pela prática.

Para além da classificação dos países, o estudo conclui que:

- os indivíduos são inconsistentes, no que diz respeito a práticas de segurança, dando prioridade ao que lhes é conveniente, e aponta como motivos para esta situação, a falta de apoio estrutural da sociedade bem como a ausência de foco na educação sobre o risco cibernético.
- os governos estabelecem prioridades e metas apropriadas na educação sobre riscos de cibersegurança, mas falham na disponibilização de recursos necessários para o seu sucesso.
- a sensibilização para a cibersegurança inicia-se demasiado tarde, carecendo de padrões e objetivos comuns de avaliação e reforço.
- os empregadores demonstram maior compromisso do que os governos com o ensino sobre o risco em cibersegurança.

Concluindo que, à medida que as pessoas se tornam cidadãos digitais globais, os países têm uma maior consciência da necessidade de aprendizagem e educação em cibersegurança. Por isso, é necessário atualizar continuamente os seus planos de cibersegurança e incorporá-los nos currículos educativos, de forma a conseguir as mudanças necessárias para uma população mais informada sobre os riscos a que está exposta online.

O artigo de Rahman et al. (2020) denominado *«The importance of cybersecurity education in school»* foi apresentado em 2020 e aborda o impacto positivo da Internet na vida das pessoas, mas também os problemas resultantes da sua utilização. Considerando que, vários estudos referidos avaliam o nível de consciencialização

entre os utilizadores como baixo ou moderado, torna-se vital tomar medidas que cultivem o conhecimento e consciencialização entre os utilizadores da Internet desde tenra idade. Este artigo analisou 25 estudos realizados entre 2011 e 2019 na área da educação, no sentido de explorar os motivos que tornam tão importante a educação sobre os riscos associados à atividade no ciberespaço e definir estratégias que se podem usar para promover e implementar a educação em cibersegurança nas escolas. O estudo considera que existem vários desafios à ciberconsciencialização nas escolas, que só poderão ser ultrapassados se os professores, pais, colegas e o governo trabalharem juntos para encontrar a melhor solução para proteger as crianças com recurso à educação. Adicionalmente, considera que os meios de comunicação social, também devem desempenhar um papel importante através da realização de campanhas de sensibilização interativas e interessantes de cibersegurança.

2.2.2 *Ciberconsciencialização nas empresas*

O artigo *«Leveraging behavioral science to mitigate cyber security risk»* de Pfleeger e Caputo (2012) aborda o problema da adoção de medidas de cibersegurança nas empresas, indicando que, na maioria dos casos onde se optou apenas pela adoção de produtos e processos tecnológicos, não se conseguiu garantir uma melhor segurança. Segundo a publicação, tal acontece porque o elemento chave para uma segurança eficaz envolve o comportamento humano e o reconhecimento da sua importância ao projetar, construir e usar a tecnologia de segurança. Este trabalho foca-se nos aspetos comportamentais, pré conceito e descobertas comprovadas e potenciais da ciência comportamental de heurísticas e modelos de ciências comportamentais, para sugerir passos para incorporar as descobertas no desenvolvimento e uso tecnológico.

O artigo McCormac et al. (2017) denominado *«Individual differences and information security awareness»* foi publicado em 2017 e teve como principal objetivo examinar a relação entre as diferenças dos indivíduos e a Consciencialização sobre Segurança da Informação (ISA). Para avaliar o nível de consciencialização, o artigo recorreu ao questionário HAIS-Q, que é baseado no modelo de conhecimento, atitude e comportamento (KAB). O estudo conclui que a consciência, a simpatia, a estabilidade emocional e a propensão a correr riscos, são fatores significativos para explicar a variância na consciencialização sobre segurança da informação dos indivíduos. Os autores realçam as importantes implicações das descobertas apresentadas nas organizações, permitindo identificar os pontos fortes e fracos e assim facilitar o

desenvolvimento de acções de treino e sensibilização, direcionadas para os seus funcionários.

O trabalho de Hadlington (2017), publicado em 2017, denominado *«Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours»*, procura explicar o modo como as diferenças individuais (comportamentos, atitudes, dependência da Internet e impulsividade) estão relacionadas com os riscos de cibersegurança em ambientes empresariais. Esta avaliação foi feita com recurso a quatro questionários online, designadamente, Abbreviated impulsiveness scale (ABIS), Online cognition scale (OCS), Risky cybersecurity behaviours scale (RScB) e Attitudes towards cybersecurity and cybercrime in business (ATC-IB). O objetivo é a identificação de preditores que forneçam um mecanismo para identificar aqueles que podem ser mais suscetíveis ao envolvimento em comportamentos de risco. O estudo conclui que: as atitudes dos funcionários em relação à cibersegurança foram negativamente correlacionadas com a frequência com que eles se envolveram em comportamentos de risco; indivíduos que se envolvem em comportamentos arriscados de cibersegurança também parecem estar ligados ao nível de uso problemático ou viciante da Internet; a impulsividade de atenção e motora apresenta-se como um preditor significativo para comportamentos de risco.

Hadlington (2017), com este trabalho, apresenta um modelo sistemático que permite determinar como os indivíduos estão ou não envolvidos no desenvolvimento de boas praticas de cibersegurança, permitindo um ajustamento da comunicação e desenvolvimento de estratégias de difusão, com informação direcionada, relevante, passível de ser posta em prática, e onde seja dado um feedback aos indivíduos, para que possam aferir o seu desempenho.

A tese de Gonçalves (2019), denominada *«O fator humano da cibersegurança nas organizações»*, estuda a influência do fator humano em contexto organizacional na cibersegurança, identificando as características e comportamentos humanos que influenciam a cibersegurança, o seu impacto nos níveis de cibersegurança e as respetivas soluções para estes comportamentos. Para a realização do estudo, foram efetuadas entrevistas individuais a peritos e investigadores em cibersegurança, com o objetivo de dar o seu contributo a nível técnico, aprofundando o estudo do fator humano da cibersegurança numa vertente prática, pela transmissão de conhecimento e sensibilização da sociedade. A tese conclui que as organizações portuguesas têm um longo caminho a percorrer, para aumentar o seu nível de maturidade em cibersegurança, sendo de esperar que passem a assumir um papel maioritariamente preventivo, olhando para a cibersegurança como um conjunto de sinergias e não

apenas como uma questão tecnológica, devendo incluir as pessoas nas suas políticas de cibersegurança. Para tal é necessário informar e sensibilizar a gestão de topo, para que existam políticas direcionadas para a cibersegurança e para que sejam alocados recursos suficientes para garantir a segurança da organização. Essa segurança passa pela consciencialização, formação e educação, estabelecendo uma cultura de cibersegurança sólida. Este trabalho salienta ainda que existem exceções, dado que existem organizações que se distinguem pelas boas práticas de cibersegurança e pela boa preparação dos seus colaboradores. No entanto, não existem soluções infalíveis, pelo que existe sempre a possibilidade de melhoria (Gonçalves, 2019).

O trabalho *«Information technology governance and cybersecurity at the board level»* de Al-Sartawi (2020), aborda a problemática da cibersegurança nas empresas e a sua importância para os seus acionistas e investidores. Considerando que, nas empresas dos EUA e médio oriente, as violações de segurança têm um custo extremamente elevado e os conselhos de administração têm de ganhar e manter a confiança dos acionistas e investidores, a cibersegurança torna-se um fator extremamente importante. Assim, é evidente a necessidade das empresas protegerem os seus dados e de os conselhos de administração incorporarem uma cultura de cibersegurança nas empresas.

Este trabalho analisa a relação entre a gestão de tecnologia de informação e o nível de cibersegurança das empresas, recolhendo dados de uma amostra de 94 empresas cotadas nos mercados de ações dos países da região do Médio Oriente e Norte da África (MENA), no ano de 2018. O estudo descobriu que existe uma relação significativa entre a gestão de segurança de informação e o nível de cibersegurança da empresa e concluiu que é de extrema importância nomear membros do conselho com conhecimento e experiência em TI, para melhores decisões, quando confrontados com ameaças e desafios cibernéticos, mas também, para entender o que as direções de departamentos de TI estão a fazer internamente e, portanto, ter conhecimento suficiente para questionar as suas ações.

O relatório «Microsoft Digital Defense Report», elaborado pela Microsoft (2020b), analisa os acontecimentos globais dos últimos 12 meses e as mudanças sem precedentes para o mundo físico e digital, onde o cibercrime é uma constante e os cibercriminosos escalaram a sua atividade. A defesa é uma tarefa complexa em constante evolução e sem fim, onde os profissionais de segurança, para criarem as suas estratégias de segurança, precisam de uma perceção diversa e mais oportuna das ameaças.

Este relatório é uma reformulação do Relatório de Inteligência de Segurança da Microsoft, publicado pela primeira vez em 2005, e reúne a perceção da Microsoft sobre estratégias de defesa online. Com a pandemia provocada pela COVID-19, alguns tipos de ataques aumentaram e os cibercriminosos mudaram de tática, sendo este relatório dedicado às novas e mais relevantes ameaças para a comunidade, focando-se em três áreas: crimes cibernéticos, ameaças de estado-nação e trabalho remoto. Adicionalmente, com base nas informações recolhidas, o relatório apresenta um conjunto de recomendações, para que as organizações adotem uma abordagem proativa, que reforce a sua segurança e resiliência e fomente a discussão sobre o que pode ser feito para combater as atividades mal-intencionadas em governos, empresas, universidades, organizações sociais e público.

O trabalho de Boletsis et al. (2021), denominado *«Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment»*, publicado em 2021, aborda a situação das pequenas e médias empresas (PME's) ao lidarem com a problemática da cibersegurança e os problemas internos que têm de enfrentar, ao tentar definir estratégias de risco em cibersegurança.

Boletsis et al. (2021) aplicaram uma abordagem de "jornada do utilizador", para modelar os comportamentos e mapear visualmente as práticas e ameaças das PMEs, juntamente com uma visualização da rede de interações entre as pessoas e a tecnologia em contexto de trabalho, e assim, permitir detetar e aumentar o nível de consciencialização sobre cibersegurança, mas também melhorar a comunicação entre especialistas em segurança e pessoal não técnico em pequenas e médias empresas (PME's).

O trabalho de Antunes et al. (2021), denominado *«Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal»*, foi publicado em 2021, e aborda o papel que a segurança da informação desempenha na gestão das empresas como forma de garantir a confidencialidade, privacidade, integridade e disponibilidade dos seus dados e informação. O artigo considera que as PMEs não colocam normalmente prioridade na gestão da segurança da informação e cibersegurança, principalmente devido ao seu tamanho, âmbito regional e familiar e recursos financeiros. Este artigo apresenta e analisa os resultados de um projeto de gestão da segurança da informação e cibersegurança, desenhado e implementado, com base na norma ISO-27001: 2013, em cinquenta PME da zona centro de Portugal. Os resultados alcançados neste trabalho mostram um claro benefício para as PMEs auditadas e intervencionadas, sendo principalmente atestado pelo aumento da robustez da gestão da segurança da informação e da ciberconsciencialização dos colaboradores.

2.2.3 *Ciberconsciencialização nas instituições de saúde*

O trabalho de Capelão e Barbosa (2018), denominado *«Cybersecurity in Healthcare: Risk Analysis in Health Institution in Portugal»*, foi publicado em 2018 e aborda a problemática da cibersegurança nas instituições de saúde e a importância da implementação da segurança da informação. Para isso, é essencial conhecer os riscos que esta área enfrenta, para posteriormente ter a capacidade de controlar, prevenir e enfrentar esses riscos. Isso só é possível com a implementação de boas práticas e adoção de métodos para prevenir os ataques.

Este trabalho apresenta como objetivo a descrição do estado de cibersegurança nas organizações de saúde e faz uma revisão da literatura existente, para entender os riscos a que têm de fazer face, as consequências e medidas para enfrentar as ameaças. O trabalho inclui uma análise de segurança a uma instituição de saúde em Portugal, para compreender o seu nível de segurança, e conclui, considerando que este tipo de instituições é propensa a ataques, uma vez que recolhem e gerem um grande volume de informações, que tem de manter de forma confidencial e garantir a sua integridade. A pesquisa, realizada na instituição de saúde, permitiu uma melhor compreensão dos cuidados e necessidades existentes e permitiu identificar algumas áreas que requerem uma atenção particular. Entre elas, Capelão e Barbosa (2018) destaca a atenção à formação e qualificação da gestão e organização das instituições e a implementação de um conjunto de controlos que garantam os objetivos específicos de segurança da organização.

O trabalho *«Avaliação das atitudes e comportamentos de cibersegurança dos profissionais de saúde em ambiente hospitalar»*, de Silva Lopes Nunes (2019), publicado em 2019 pela Escola Superior de Tecnologia da Saúde de Lisboa, procura compreender qual o nível de conhecimentos dos profissionais de saúde em relação à segurança da informação e identificar riscos e ações que possam ser tomadas para aumentar a sensibilização destes profissionais em Portugal, avaliando as suas atitudes e comportamentos de cibersegurança. Para atingir este objetivo, o autor faz a tradução e aplicação das escalas de atitudes em relação à cibersegurança em ambiente empresarial (ATC-IB) e comportamentos arriscados em cibersegurança (RScB) de Hadlington, apresentando os resultados observados e um conjunto de conclusões que podem servir de termo de comparação com outras realidades.

2.2.4 *Ciberconsciencialização em organismos de estado*

O artigo *«Utopia, liberdade e soberania no ciberespaço»* de Fernandes (2012) discute os desafios que o ciberespaço e o risco de ciberataques acarreta para a soberania dos estados e para a liberdade dos cidadãos. Nos primórdios da Internet, dominava uma liberdade anárquica, que progressivamente tem dado lugar a mecanismos de controlo e afirmação de soberania dos estados, através da criação de "fronteiras" no ciberespaço. Esta tendência assume diversas formas, podendo ser detetada tanto em estados autoritários como nas democracias, onde cada um desenvolve as suas "Políticas de Informação" e estratégias integradas. O objetivo é aumentar os seus recursos de informação, garantir a segurança e a proteção da sua infraestrutura de informação e potenciar o livre acesso e a utilização do espaço onde ela circula. Esta tendência, embora sob formas diferentes, pode ser também encontrada na organização das forças armadas, com a criação de ciber-comandos, e nas OIG ligadas à segurança e defesa, como a NATO, onde se passou a incluir a ameaça de ciberataques no conceito estratégico.

O desenvolvimento de estruturas e capacidades nos domínios da cibersegurança e da ciberdefesa é, por isso, uma realidade que este trabalho analisa, com o objetivo de procurar avaliar, em que medida a resposta de segurança dos Estados ao crescente risco de ciberataques ou de uma ciberguerra, põe em causa a liberdade do cidadão.

O relatório, com a designação Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity da ENISA (2019), aborda os aspetos humanos da cibersegurança e aborda a pesquisa existente sobre o comportamento humano (também denominada "ciência do comportamento"), que abrange uma ampla gama de disciplinas, com o único aspeto unificador de investigar o ator humano. O artigo inclui não apenas a psicologia e a sociologia, mas também a etnografia, a antropologia, a biologia humana, a economia comportamental e outroa assuntos que tenham o ser humano como ponto principal.

O relatório conclui que as ameaças cibernéticas existem em todas as organizações cujos negócios dependem de uma infraestrutura de TI e da Internet, mas a gestão da maioria das organizações viu, até agora, o problema como técnico. Adicionalmente, muitas das políticas de segurança adotadas causam atrito com a gestão do negócio e, quando isso acontece, a maioria dos funcionários coloca a "produtividade em primeiro lugar".

Assim o relatório ENISA (2019) sugere que os gestores tenham um papel ativo para garantir um comportamento adequado relativamente à segurança da informação,

dando o exemplo, tomando responsabilidades e gerindo a organização de modo a auxiliar gestão da cibersegurança e segurança da informação.

O «Relatório Cibersegurança em Portugal – Sociedade 2020», publicado pelo Cibersegurança Portugal (2020), apresenta a evolução da cibersegurança em Portugal, com base num conjunto de indicadores que se enquadram em três temas centrais: atitudes, comportamentos e a educação e sensibilização. O relatório aborda os comportamentos individuais e organizacionais, com base em três inquéritos (um do Eurostat, sobre as Empresas, e dois da Direção-Geral de Estatísticas de Educação e Ciência - DGEEC, sobre a Administração Pública Central e Regional e sobre as Câmaras Municipais). Este relatório pretende olhar, de forma mais aprofundada, para a realidade portuguesa e desenvolver uma compreensão abrangente e sintética sobre a vertente social da cibersegurança no país. Disponibiliza uma base de informação para as decisões estratégicas, quanto à educação e sensibilização dos indivíduos, e apresenta um conjunto de conclusões e comparações com a EU e recomendações de ação para a Administração Pública, empresas e utilizadores em relação à cibersegurança.

O artigo *«European strategy and legislation for cybersecurity: implications for Portugal»* de Carvalho et al. (2020), aborda o problema crescente dos ciberataques e a proliferação de dispositivos e tarefas que fazem parte da nossa vida e que estão ligados à Internet. Com o crescente número de vítimas destes ataques, também tem crescido a preocupação geral sobre cibercrime e os ciberataques. Neste contexto, a União Europeia lidera o esforço de regular a defesa contra as ciberameaças, tanto a nível normativo/legal como estratégico, e consequentemente em Portugal. Este artigo apresenta a Estratégia e Legislação Europeia para a Cibersegurança e como esta estratégia se aplica e envolve Portugal.

2.2.5 *Outras*

O artigo *«Understanding the human dimension of cyber security»*, realizado por Mittal (2015) na India, analisa a interação entre humanos e computadores e explora as motivações dos comportamentos dos utilizadores, procurando determinar se existe uma base psicológica para os comportamentos, e procura identificar de que forma influenciam a segurança nos sistemas de computadores. O artigo conclui que o aspeto mais importante e dinâmico da interação entre humanos e computadores é o comportamento dos utilizadores, variando no espaço e no tempo, e sendo

influenciados por fatores psicológicos regidos, entre outros, pelo comportamento dos pares, crenças normativas e pressões sociais.

O trabalho de Sen (2018), com a designação *«Challenges to cybersecurity: Current state of affairs»*, aborda o aumento do investimento em iniciativas de cibersegurança e a tendência de aumento dos incidentes de violação de dados, infecções por malware e ciberataques, identificando um conjunto de desafios técnicos, económicos, jurídicos e comportamentais que continuam a obstruir qualquer esforço significativo para alcançar uma cibersegurança razoável. O artigo resume, ainda, as várias iniciativas recentes realizadas nos Estados Unidos por várias partes interessadas, para enfrentar estes desafios, e destaca as limitações dessas iniciativas.

O artigo *«Enhancing security behaviour by supporting the user»*, de Furnell et al. (2018), aborda a problemática da comunicação na manutenção da segurança. Este trabalho salienta que a função dos utilizadores na manutenção da segurança é regularmente enfatizada, mas afirma que geralmente não é correspondida de forma adequada pela equipa de gestão de TI. Os autores consideram que é frequente os utilizadores receberem orientação insuficiente para escolhas e decisões de segurança. Este trabalho procura formas de apoio e investiga o seu efeito prático, baseando-se no resultado de dois estudos experimentais que investigaram as variações nas passwords, com base no feedback fornecido.

O primeiro estudo examina a diferença entre as senhas dos utilizadores sem orientação e dos que recebem orientações e formas alternativas de feedback na definição das suas passwords. O segundo estudo avalia a influência das variações na forma das mensagens de feedback nas passwords escolhidas pelos utilizadores. O estudo conclui que se verificou uma queda de 30% nas opções de passwords fracas, entre o uso não guiado e guiado, e 10% de melhoria nas escolhas guiadas. Da mesma forma, ao disponibilizar informações mais ricas, os utilizadores ficam mais motivados a fazer melhores escolhas e a mudar as passwords inicialmente fracas. O estudo conclui ainda que, embora as descobertas apresentadas estejam centradas nas passwords dos utilizadores, existem benefícios na aplicação desta estratégia em outras áreas de segurança onde os utilizadores têm comportamentos menos corretos.

A Microsoft, enquanto fornecedor de tecnologia, também tem procurado contribuir para a consciencialização dos utilizadores. No «Empowering and securing your Firstline Workforce eBook», aborda a realidade mundial, onde os governos reconhecem que a preparação de uma força de trabalho de próxima geração com as habilidades necessárias é a chave para permitir maiores oportunidades e melhor qualidade de vida. Esses objetivos estão alinhados com o Objetivo de Desenvolvimento

Sustentável das Nações Unidas (ODS) nº 8 (194 países assinaram), propondo-se o crescimento económico sustentado, inclusivo e sustentável, o emprego pleno e produtivo e trabalho digno para todos. É, por isso, essencial transformar a maneira como os alunos aprendem e como os educadores ensinam, e alinhar-se as habilidades que os empregadores desejam para atingir estes objetivos. Com um grande foco em tecnologia e ampla experiência no setor público, a Microsoft trabalha com organizações governamentais e não governamentais (ONGs), escolas, educadores e empresas, para desenvolver as habilidades de tecnologia dos alunos e capacitar e ajudar os trabalhadores de hoje a adquirirem as habilidades de que precisam para amanhã. Este ebook apresenta uma lista de programas e soluções da Microsoft, que permitem o desenvolvimento de habilidades de TI do século XXI para os jovens, estudantes mais avançados e adultos.

2.3 SUMÁRIO

A interação entre os seres humanos e dispositivos eletrónicos (computadores, telemóveis, tablets ou outros) é dinâmica, pois o comportamento dos utilizadores varia no espaço e no tempo, sendo influenciado por múltiplos fatores, inclusive os psicológicos. Assim, uma abordagem única na mitigação de riscos de cibersegurança não apresenta os resultados esperados.

A literatura apresentada evidencia a importância da ciberconsciencialização, mas também a necessidade de uma boa comunicação com os utilizadores.

Neste contexto, o presente relatório de projeto traduz e adapta ao contexto educacional as escalas publicadas em *«Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours»* por Hadlington (2017), procurando utilizar este modelo sistemático para determinar como os alunos estão ou não envolvidos no desenvolvimento de boas práticas de cibersegurança, com o objetivo de dotar as instituições de um mecanismo que lhes permita um ajustamento da comunicação e desenvolvimento de estratégias de difusão, com informação direcionada.

3

DESENVOLVIMENTO

Neste capítulo, aborda-se a metodologia de trabalho, as decisões envolvidas na realização e os resultados da realização. Na secção 3.1, é apresentado o resultado do trabalho realizado na construção das novas escalas de CsB-S (Cybersecurity Behaviors In Schools) e CsA-S (Cybersecurity Attitudes In Schools) e as decisões envolvidas na construção do questionário de Auto-diagnótico e do plano aula. As secções seguintes apresentam o resultado do trabalho realizado, designadamente a nova escala de atitude (secção 3.2), a nova escala de comportamentos (secção 3.3), o plano de aula, com as as motivações associadas às decisões tomadas e o trabalho resultante (secção 3.4) e o questionário de autodiagnóostico, com as motivações e decisões tomadas e o resultado obtido (secção 3.5).

A concluir este capitulo temos a secção 3.6, que apresenta o resumo do trabalho realizado enquadrando-o com os objectivos deste trabalho.

3.1 METODOLOGIA DE TRABALHO

Esta secção descreve a metodologia adotada na realização deste projeto, descrevendo os passos tomados no processo de adaptação das escalas para contexto escolar (subsecção 3.1.1), as decisões envolvidas na elaboração e criação do questionário de auto-diagnóstico (subsecção 3.1.2) e na criação do plano de aula (subsecção 3.1.3).

3.1.1 *Adaptação das escalas*

Este trabalho pretende avaliar o nível de consciencialização e identificar comportamentos de risco dos alunos online, dotando as escolas de uma ferramenta de avaliação que lhes permita o desenvolvimento de conteúdos personalizados. A avaliação será feita pela análise dos comportamentos e atitudes dos alunos, com recurso a questionários. Tendo em mente este objetivo, definiu-se o plano do trabalho a realizar, desde a preparação dos questionários até à sua aplicação em contexto escolar, seguindo as normas e boas práticas existentes, designadamente a tradução

para Português, o ajuste das perguntas para o contexto em que foram usadas e ainda a validação e recolha de *feedback* por parte de peritos.

A Figura 2 representa esquematicamente o plano de trabalho definido.

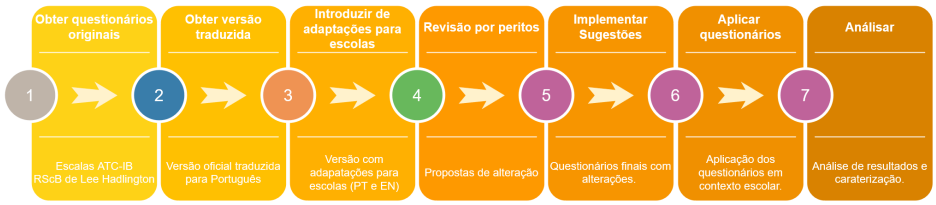


Figura 2: Abordagem adotada para a construção dos questionários

De seguida, passo a apresentar as tarefas realizadas em cada uma das fases do plano definido.

3.1.1.1 *Fase1 - Obter questionários*

Numa primeira fase, procedeu-se ao levantamento da literatura existente e escalas que avaliem atitudes e comportamentos publicadas. Analisadas as opções e verificada a aplicabilidade em contexto escolar, optou-se pela adaptação das escalas validadas *Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB)* e *Risky Cybersecurity Behaviours Scale (RScB)* de Hadlington, 2017. Para isso, foi dirigido um pedido de autorização de utilização ao autor (disponível em anexo: A.3), tendo-se dado início ao trabalho de adaptação das escalas, após a receção da resposta a autorizar a sua utilização, que inclui uma sugestão de abordagem (disponível no anexo A.4).

3.1.1.2 *Fase 2 - Versão traduzida das escalas*

Uma vez recebida a autorização e registadas as sugestões do autor, fez-se uma pesquisa por versões traduzidas e validadas das referidas escalas, tendo identificado um trabalho de Silva Lopes Nunes (2019), onde são apresentadas versões traduzidas e validadas para língua portuguesa.

3.1.1.3 *Fase 3 - Adaptação das escalas*

Dispondo da versão em Inglês das escalas e da versão traduzida e validada em Português, deu-se início ao processo de adaptação das escalas para contexto escolar. Considerando que estas escalas continham perguntas que se referiam ao contexto organizacional e que não se enquadravam nos conhecimentos dos alunos, e tendo em

conta a sugestão do autor das escalas aquando da sua autorização para a utilização neste trabalho, decidiu-se substituir as perguntas de gestão organizacional por perguntas 'ajustadas' à realidade da população estudantil.

As novas perguntas enquadram-se no contexto da cidadania digital do uso responsável da tecnologia, da Internet e dispositivos digitais. Foram também feitos ajustes para que as perguntas se enquadrassem na realidade institucional e no tipo de relações dos alunos. As perguntas substituídas e os ajustes nas perguntas da "Escala de Atitudes" são descritos na secção 3.2, e na "Escala de Comportamentos" na secção 3.3.

3.1.1.4 *Fase 4 - Revisão por peritos*

Seguindo as normas e boas práticas existentes, uma vez concluído o trabalho de adaptação inicial das escalas, solicitou-se a colaboração de peritos, com o objetivo de recolher *feedback*, opiniões e sugestões de melhoria.

Construídas as novas escalas, solicitou-se então a colaboração de 3 peritos. Os peritos convidados foram o Professor Baltazar Rodrigues, o Professor Carlos Rabadão e o Professor Lee Hadlington.

O Professor Baltazar Rodrigues é Inspetor da Polícia Judiciária, com 28 anos de carreira, na área do combate à criminalidade informática. Licenciado em Engenharia Informática pela Universidade Autónoma de Lisboa (UAL), pós-graduado em Direito e Cibersegurança pela Faculdade de Direito da Universidade de Lisboa (FDUL) e, atualmente, mestrando em Guerra de Informação, pela Academia Militar (AM), e detentor de diversas certificações internacionais em análise digital forense. É Professor adjunto convidado no curso de mestrado em cibersegurança e informática forense, no Instituto Politécnico de Leiria.

O Professor Carlos Rabadão é doutorado em Engenharia Informática, com o tema Segurança em Redes com Diferenciação de Serviços, pela Faculdade de Ciências e Tecnologia da Universidade de Coimbra, tendo obtido o grau de mestre em Electrónica e Telecomunicações, pela Universidade de Aveiro, e a licenciatura em Engenharia Electrotécnica, área de Telecomunicações e Electrónica, pela Faculdade de Ciências e Tecnologia da Universidade de Coimbra. É Professor Coordenador com contrato de trabalho em funções públicas, por tempo indeterminado, na área científica de Tecnologias de Segurança, afeto ao Departamento de Engenharia Informática da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, investigador do Centro de Investigação em Informática e Comunicações

do Instituto Politécnico de Leiria e membro do Laboratório de Cibersegurança e Informática Forense do Instituto Politécnico de Leiria.

Por fim, o Professor Lee Hadlington é psicólogo licenciado, conferencista sênior em ciberpsicologia e membro do grupo de pesquisa em ciberpsicologia. É o atual co-líder do curso de mestrado em Ciberpsicologia e ensina na área da Ciberpsicologia. Os convites de colaboração encontram-se disponíveis para consulta no anexo A.5.

Com o intuito de tentar cumprir o plano de trabalhos definido para o projeto e evitar atrasos, foi solicitado que os contributos fossem submetidos até 24/12/2021, tendo á data definida sido rececionados os contributos do Professor Baltazar Rodrigues e do Professor Carlos Rabadão (disponíveis para consulta no anexo A.6).

3.1.1.5 *Fase 5 - Implementar sugestões*

Terminada a fase de recolha de opiniões, propostas e observações dos especialistas (Propostas e observações do Professor Baltazar Rodrigues disponiveis no anexo A.6.1, e do Professor Carlos Rabadão no anexo A.6.2), deu-se inicio ao processo de ajuste final das escalas, doravante designadas de Cybersecurity Behaviors In Schools (CsB-S) (descrita em 3.3) e Cybersecurity Attitudes In Schools (CsA-S) (descrita em 3.2).

Os ajustes efetuados em função dos contributos dos especialistas encontram-se disponíveis para consulta no anexo A.7.1 e A.7.2, tendo as perguntas destacadas com uma cor sido alvo de ajuste.

As perguntas dos questionários de comportamentos (CsB-S) transitam do questionário original com ajuste na tradução para língua portuguesa e com a inclusão de alguns exemplos. A única exceção é a pergunta 5 onde se propôs a substituição da pergunta original pela seguinte: *"Insere informação de pagamento em jogos "Freemium", que são gratuitos mas que oferecem benefícios mediante pagamento"*. Considerando as observações e tendo em conta a relevância para o contexto, uma vez que os jovens também utilizam plataformas de jogos pagas online, decidiu-se reverter para a pergunta original *"Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita"*.

No questionário de Atitudes (CsA-S), as perguntas foram ajustadas para refletir o tipo de organização onde se pretende aplicar os questionários e alterações no sentido de tornar menos ambígua a interpretação das perguntas.

As perguntas 1, 6, 11, 12, 20, 25 são perguntas inseridas no contexto organizacional e, considerando que não se pretende caraterizar os comportamentos organizacionais

e considerando a sugestão do autor das escalas aquando da sua autorização para a utilização neste trabalho, decidiu-se manter a substituição das perguntas por outras enquadradas no contexto da cidadania digital do uso responsável da tecnologia, da Internet e dispositivos digitais.

3.1.1.6 *Fase 6 - Aplicar questionários*

Nesta fase, fez-se o pedido de aplicação do questionário em contexto escolar (anexo A.1) e realizou-se o trabalho de preparação que precede a aplicação com a inserção das perguntas, alojamento e publicação online na plataforma LimeSurvey. Um vez recebida a autorização da instituição (anexo A.2) e, terminado este trabalho de preparação, procedeu-se à aplicação no estabelecimento de ensino particular e cooperativo da cidade de Leiria, designadamente, o Colégio Conciliar de Maria Imaculada (CCMI).

Nesta fase foi também elaborado um texto de conformidade com o RGPD para o tratamento de dados que teve de ser aceite para que fosse possível a visualização e resposta dos questionários (disponível para consulta no anexo A.10).

O preenchimento dos questionários foi realizado em regime presencial, durante uma aula de TIC com cada uma das turmas selecionadas nos dias 09/04/2021, 13/04/2021 e 15/04/2021. A aula iniciou-se com a apresentação e os objetivos dos questionários, sendo depois disponibilizados e respondidos pelos alunos tal como descrito no plano disponível no anexo C.1. É de notar que os encarregados de educação foram previamente informados, dos objetivos dos questionários por mensagem de e-mail remetida pela escola. Tiveram ainda de autorizar os seu educandos a participar no estudo. Os questionários de atitudes e comportamentos aplicados em contexto escolar encontram-se disponíveis para consulta, respetivamente no anexo A.8, e A.9.

3.1.1.7 *Fase 7 - Análise*

Uma vez terminada a recolha das respostas, deu-se início ao processo de análise com o intuito de identificar comportamentos, tendências e más práticas, realizadas online, em contexto escolar e em casa, dos alunos a terminar o 2º e 3º ciclos. A análise foi feita com base nos dados de caraterização recolhidos dos participantes por género, ano de frequência e formação académica do agregado familiar (pai e mãe) e nas perguntas da investigação elencadas na tabela 1:

Investigação procura responder às seguintes perguntas	
1	Existe algum indicador de atitudes e comportamentos que esteja claramente relacionado com o género?
2	Com base nas respostas é possível identificar uma diferença no nível de consciencialização e capacidade de resposta ao risco com base no ano que frequentam?
3	As habilitações académicas dos pais têm associação nos comportamentos de risco dos alunos(filhos)?
4	Os alunos manifestam algum nível de preocupação com a sua privacidade e a consequência da divulgação dos seus dados?
5	As atividades atitudes e comportamentos online dos alunos são tendencialmente positivas ou negativas?
6	Qual a perceção dos alunos sobre a informação disponibilizada pela Escola sobre cibersegurança ?
7	Em situações de contactos por parte de estranhos, os alunos estão suficientemente atentos,despertos e informados para tomar todas as precauções ?
8	Os alunos tem consciência das consequências que as suas atitudes e comportamentos trazem para a instituição?
9	Os alunos compreendem as motivações dos cibercriminosos e o que os leva a efetuar ataques e as suas táticas mais comuns?
10	Os alunos acreditam nas competências das entidades policiais e dos serviços técnicos da Instituição?
11	Os alunos preocupam-se em proteger os seus equipamentos e os dados?
12	Os alunos estão conscientes das consequências da utilização de software de fontes não oficiais e de não respeitarem os direitos autor?

Tabela 1: Perguntas da investigação

Os resultados obtidos e as respostas às perguntas de investigação são apresentados no capítulo 4.

3.1.2 *Questionário de Auto-diagnóstico*

A criação do questionário de Auto-diagóstico tem como objetivo disponibilizar uma ferramenta aos alunos que lhes permita, de forma autónoma, avaliar e melhorar os seus conhecimentos e mitigar as possíveis lacunas que possam ser identificadas. Para isso, pretende-se que o questionário apresente um conjunto de perguntas que possibilite um autodiagnóstico e disponibilize *feedback* dos conhecimentos e sugestões de leitura.

De forma sucinta, o trabalho de preparação pode ser subdividido em cinco fases descritas na figura 3.

Figura 3: Fases da elaboração do questionário de auto-diagnóstico

O trabalho desenvolvido em cada uma das fases é descrito nas subsecções 3.1.2.1 a 3.1.2.5.

3.1.2.1 *Fase 1 - Áreas a abordar*

Na fase inicial, começou-se por definir o método de classificação e organização das perguntas com o intuito de ser tão abrangente quanto possível, tendo-se optado por uma classificação das perguntas por tipo de incidente, recorrendo à organização da taxonomia de referência de incidentes de segurança e utilizada pela rede nacional de CSIRT (CSIRT – Grupo de Trabalho Taxonomia, 2020), disponível para consulta no anexo B.1.

Os incidentes são classificados por uma classe (num total de 10) e por tipo de incidente. As dez classes de incidentes são: "Conteúdo Abusivo", "Código Malicioso", "Recolha de Informação","Tentativa de Intrusão", "Intrusão", "Disponibilidade", "Segurança da Informação", "Fraude", "Vulnerabilidade"e "Outro", tendo cada um conjunto de tipos de incidentes definido.

3.1.2.2 *Fase 2 - Base de dados de perguntas*

Tendo em conta que esta taxonomia, dentro de cada classificação faz uma separação por tipos de incidentes, na segunda fase definiu-se um conjunto de perguntas a incluir no questionário por cada tipo de incidente das classes definidas. Poderão ser adicionadas novas perguntas para contemplar outras áreas identificadas como problemáticas, e assim fazer face a situações emergentes melhorando a base de dados de perguntas.

A base de dados de perguntas criadas encontra-se disponivel para consulta no anexo B.2.

3.1.2.3 *Fase 3 - Texto de feedback*

Definido o conjunto inicial de perguntas a disponibilizar, na terceira fase definiu-se a informação de *feedback* a dar aos alunos.

Definiu-se a disponibilização de um *feedback* quantitativo referente ao seu desempenho geral e um *feedback* por pergunta a disponibilizar quando a resposta dada não é a correta.

O texto de feedback de cada pergunta, é composto por texto explicativo e, por vezes acompanhado de links de instituições oficiais com informação que aborde a

problemática em questão, que permitirá esclarecer qual ou quais as práticas mais seguras a adotar.

3.1.2.4 *Fase 4 - Estratégia de seleção de perguntas e feedback*

De seguida, tendo em conta o número elevado de perguntas resultante para abranger os tipos de incidentes definidos na taxonomia, foi necessário definir uma estratégia de seleção de perguntas a incluir no questionário a apresentar aos alunos, o seu número e o tipo e forma de *feedback* a disponibilizar. As decisões tomadas nesta fase estão documentadas em detalhe na secção 3.5.

3.1.2.5 *Fase 5 - Publicação*

Na fase de publicação, tratou-se de toda a logística de preparação e desmobilização online em plataforma para o efeito aos alunos, ficando disponível para acesso sempre que o aluno o desejar.

O questionário de auto-diagnóstico foi disponibilizado num servidor Linux com a plataforma moodle (versão 3.9) de uso interno da instituição. Numa primeira fase foram criadas as categorias e perguntas da base de dados de perguntas, seguindo a lista previamente definida disponível no anexo B.2. Só depois se deu inicio ao processo de configuração do questionário, definindo o critério de seleção das perguntas, forma de feedback e parametrização, tal como definido na secção 3.5.

A Figura 4 apresenta a composição do questionário, apresentando o nome das categorias (de acordo com a taxonomia de referência para classificação de incidentes de segurança da rede nacional de CSIRT) e o número de perguntas a incluir por categoria.

Figura 4: Composição do questionário de autodiagnostico

O anexo B.3 apresenta um exemplo de questionário gerado e o anexo B.4, o mesmo questionário com respostas corretas e erradas onde é possível ver a informação de feedback disponibilizada.

3.1.3 *Planos de aula*

Os planos foram elaborados em função das necessidades observadas tendo em vista uma intervenção pedagógica nas áreas identificadas como mais problemáticas. Integrados num plano de ação abrangente com o intuito de consciencializar para a cibersegurança e mitigar atitudes e comportamentos de risco dos alunos do ensino básico. Pretende-se que sejam parte de uma unidade curricular a incluir na disciplina de Tecnologias de Informação e Comunicação (TIC) e/ou Educação para a Cidadania.

Os planos apresentados pretendem ser um instrumento de trabalho do professor. Definem um conjunto de objetivos e práticas pedagógicas para os atingir (I.Arends, 2008). Prende-se que sejam uma proposta de guia com material de estudo para o professor que precise de pesquisar e refletir sobre os assuntos a serem lecionados. Apresentam uma proposta de estratégias de ensino e aprendizagem para promover um ambiente de sala de aula que torne agradável aprender e contribuir para o aumento da motivação, do envolvimento e da autonomia dos alunos perante a aprendizagem.

Os planos elaborados incluem o tema e duração prevista da aula, os objetivos que se pretende alcançar no final e o conjunto de conteúdos a transmitir.

São ainda abordadas a metodologia recomendada a utilizar pelo professor para transmitir os conteudos relativos ao tema, e a forma como se pretende manter a concentração e atenção dos alunos. O plano assenta em aulas expositivas e debate, com recurso a animações e exemplos práticos. O plano da aula define igualmente a forma de avaliação que pretende avaliar, nomeadamente ao nível da assimilação de conteúdos por parte dos alunos (Silva e Lopes, 2016). Para isso, é disponibilizado o link de acesso aos questionários *Cybersecurity Behaviors In Schools (CsB-S)* e *Cybersecurity Attitudes In Schools (CsA-S)* e, no caso de plano de aula de *"Sensibilização para os comportamentos e atitudes corretas de prevenção e combate em cibersegurança"*, o questionário de autodiagnóstico. A avaliação das respostas dadas pelos alunos permitirá ao professor avaliar o nível de consecução dos objetivos definidos.

É igualmente definida uma secção de referências e fontes utilizadas para a elaboração dos planos (caso se aplique) e outras referências para partilhar com os alunos, permitindo que aprofundem os conteúdos. A secção 3.4, apresenta informações adicionais sobre os planos de trabalho desenvolvidos.

3.2 ESCALA DE ATITUDES

Como resultado do trabalho de adaptação, temos a nova escala designada de CsA-S *(Cybersecurity Attitudes In Schools)* baseada no trabalho de Hadlington (2017) com 25 perguntas. A tabela 2 mostra as perguntas que a constituem e, em seguida, a justificação das escolhas feitas.

Cybersecurity Attitudes In Schools (CsA-S)	
ID#	ITEM#
A1	Acredito que é seguro ignorar avisos de atualizações do software do computador.
A2*	Estou ciente do meu papel em manter a escola protegida de potenciais ciberameaças.
A3*	Penso que todos na escola têm um papel a desempenhar na proteção contra as ciberameaças.
A4	É difícil saber como posso ajudar a proteger a escola do cibercrime.
A5	Não tenho as competências necessárias para proteger a escola do cibercrime.
A6*	Acredito que a informação pessoal não deve ser revelada online, nomeadamente quem sou, onde vivo ou que escola frequento.
A7	Os sistemas informáticos oferecem toda a proteção de que uma escola necessita.
A8	Creio que denunciar o cibercrime é uma perda de tempo.
A9	As autoridades de segurança não tem meios para combater o cibercrime de forma eficaz.
A10	Creio que os cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger.
A11	Faria o download de material abrangido por direitos de autor (imagens, documentos, vídeos).
A12*	Acredito que, quando visualizo conteúdos relacionados com violência em contexto escolar, posso estar a promover a sua partilha e comentários.
A13	Receio que, se denunciar um ciberataque às autoridades, isso vá prejudicar a reputação da escola.
A14	Penso que poderá ser feito mais para dar a conhecer/divulgar/sensibilizar os riscos do cibercrime à comunidade educativa.
A15*	Estou a par das regras de utilização dos recursos informáticos da Escola e tento segui-la.
A16	Se ocorrer um ciberataque, não sei/não saberei como denunciá-lo.
A17	Não acho que seja minha responsabilidade denunciar um ciberataque que tenha sido lançado a partir da Escola.
A18	Não presto atenção à informação disponibilizado pela Escola sobre as ameaças do cibercrime.
A19*	Confio na minha capacidade de detetar/identificar sinais de um ciberataque.
A20*	Acredito que quando aparecem conteúdos inapropriados online, devo pedir ajuda a um adulto.
A21*	Sinto que qualquer pessoa da escola está em risco de manipulação por ciber "vigaristas e burlões".
A22	Penso que os cibercriminosos e hackers apenas atingem uma escola quando têm muito a ganhar do ponto de vista financeiro.
A23	Apenas as grandes empresas e organizações são alvo dos hackers e cibercriminosos.
A24	Acredito que apenas as instituições que utilizam meios de pagamento online estão em risco de serem vítimas de um ciberataque.
A25	Penso que tenho o direito de estar sempre online, com acesso a todos os serviços da Internet.

Tabela 2: Escala Cybersecurity Attitudes In Schools (CsA-S) em Português

Uma pontuação alta na escala CsA-S indica um envolvimento positivo na cibersegurança, enquanto uma pontuação mais baixa indica uma atitude negativa e um envolvimento mais baixo. As entradas assinaladas com o símbolo `'*'` na tabela, indicam perguntas com pontuação invertida, sendo indicadores de atitudes que indiciam um envolvimento positivo.

A escala de atitudes é composta por vinte e cinco perguntas, baseadas na escala ATC-IB de Hadlington (2017), tendo as perguntas sido adaptadas em termos linguísticos ao contexto de aplicação. Foram também substituídas as perguntas que se referiam ao contexto organizacional, no âmbito da gestão, por não se enquadrarem nos conhecimentos dos alunos e, como sugestão do autor das escalas aquando da sua autorização, para a utilização neste trabalho.

Estas foram substituídas por perguntas que se enquadram no contexto da cidadania digital do uso responsável da tecnologia, da Internet e dispositivos digitais.

As perguntas em causa são respetivamente:

- A pergunta 1 onde passa a constar *"Acredito que é seguro ignorar avisos de atualizações do software do computador"* onde se pretende verificar se os alunos têm uma atitude positiva ou negativa perante os pedidos de atualização que lhes são apresentados e que podem comprometer a segurança.
- A pergunta 6 que passa a ser *"Acredito que a informação pessoal não deve ser revelada online, nomeadamente quem sou, onde vivo ou que escola frequento"* procurando identificar a atitude dos alunos online, em relação à proteção de dados.
- A pergunta 11 *"Faria o download de material abrangido por direitos de autor (imagens, documentos, vídeos)"* pretende identificar a consciencialização para a problemática dos direitos de autor e a atitude que tomam face à informação disponível online abrangida.
- A pergunta 12 *"Acredito que, quando visualizo conteúdos relacionados com violência em contexto escolar, posso estar a promover a sua partilha e comentários"* procura determinar o tipo de atitude adotada pelos alunos quando confrontados com a situação e as consequências das suas atitudes face à violência em contexto escolar.
- A pergunta 20 *"Acredito que quando aparecem conteúdos inapropriados online, devo pedir ajuda a um adulto"* pretende ver o tipo de atitude adotada pelos alunos quando confrontados com conteúdos online inapropriados.

- E a pergunta 25 *"Penso que tenho o direito de estar sempre online, com acesso a todos os serviços da Internet"* pretende determinar se os alunos apresentam algum tipo de dependência da Internet e se existe algum vínculo entre o vício em Internet e o potencial de se envolver em comportamentos arriscados de cibersegurança.

Esta escala é, portanto, composta por perguntas sobre as atitudes que levam as instituições a serem atacadas como resultado de práticas inadequadas e perguntas no contexto da cidadania digital do uso responsável da tecnologia, da Internet e dos dispositivos digitais.

Para a avaliação é utilizada uma escala de Likert que varia de 0 a 6 (0 = Nunca,1 = 1 a 2 vezes por semestre, 2 = 1 a 2 vezes por trimestre ,3 = 1 a 2 vezes por mês ,4 = 1 a 2 vezes por quinzena ,5 = 1 a 2 vezes por semana e 6 = Diariamente), quantificando a frequência com que se envolvem em comportamentos específicos durante um período de 6 meses anteriores à data de acesso ao questionário.

3.3 ESCALA DE COMPORTAMENTOS

Esta nova escala, designada de CsB-S *(Cybersecurity Behaviors In Schools)* resulta, do trabalho de adaptação da escala *Risky Cybersecurity Behaviours Scale (RScB)* de Hadlington (2017) e é composta por 20 perguntas transcritas na tabela 3.

Cybersecurity Behaviors In Schools (CsB-S)	
ID#	ITEM#
B1	Partilhar palavras-passe com colegas.
B2	Usar ou criar palavras-passe demasiado simples. (ex.: nome de familiar, data de nascimento, apelidos, sequencias de carateres)
B3	Usar a mesma palavra-passe para diferentes websites.
B4	Usar sistemas de armazenamento online (cloud) para partilhar ou guardar informação pessoal e sensível.
B5	Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita.
B6	Usar redes Wi-Fi de acesso livre (públicas).
B7	Confiar nos conselhos de um amigo ou colega próximo sobre aspetos de segurança online.
B8	Descarregar software/apps antivírus gratuito de fontes desconhecidas.
B9	Desativar o antivírus do computador para que possa descarregar informação de websites.
B10	Utilizar a pen drive pessoal com a finalidade de transferir informação para os computadores da Escola.
B11*	Verificar regularmente as atualizações de software do smartphone/tablet/portátil/PC.
B12	Descarregar conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas.
B13	Partilhar a sua localização nas redes sociais. (Fotos, local de férias...)
B14	Aceitar pedidos de amizade em redes sociais porque reconhece fotos.
B15	Clicar em links em emails recebidos de uma fonte desconhecida.
B16	Enviar informação pessoal a estranhos pela Internet (contactos nas redes sociais, dar números de telefone ou email para obter códigos de download ou prémios, etc..) .
B17	Clicar em links de email enviados por amigos próximos ou por colegas de Escola.
B18*	Verificar atualizações para quaisquer antivírus que tenha instalado.
B19	Descarregar informação e material de websites para o computador sem verificação da veracidade.
B20	Guardar informação pessoal, de familiares e amigos no dispositivo eletrónico pessoal. (por ex., smartphone/tablet/portátil)

Tabela 3: Escala Cybersecurity Behaviors In Schools (CsB-S) em Português

A obtenção de uma pontuações mais altas na escala CsB-S indica que o indivíduo está envolvido em comportamentos de cibersegurança mais arriscados.

As entradas assinaladas com o símbolo `'*'` na tabela, indicam perguntas consideradas indicadores positivos, sendo indicadores de comportamentos mais seguros dos indivíduos.

A escala de comportamentos é composta por vinte perguntas, baseadas na escala de RScB de Hadlington (2017), tendo as perguntas do novo questionário sido adaptadas ao contexto de aplicação do questionário.

A escala foi adaptada para refletir um amplo espectro de comportamentos em relação à cibersegurança e ao cibercrime em contexto educacional. A escala de avaliação é pontuada usando uma escala Likert de 4 pontos; (4) Discordo totalmente, (3) Discordo, (2) Concordo, (1) Concordo totalmente.

3.4 DEFINIÇÃO DO PLANO DE AULA

Com o objetivo de auxiliar a escola na sua tarefa de ciberconsciencialização e no âmbito deste trabalho, foram também desenvolvidos dois planos de trabalho. O primeiro, com uma duração prevista de 60 minutos, é direcionado para os alunos de 6.º e 9.º ano e planifica a apresentação e aplicação dos questionários *(Cybersecurity Behaviors In Schools* (CsB-S) e *Cybersecurity Attitudes In Schools* (CsA-S)) em contexto de sala de aula (disponível no anexo C.1), para posterior análise. O segundo é um plano para uma aula ou ação de sensibilização planeada para 90 minutos, direcionado para os alunos de 2º e 3º ciclos, onde são abordadas as principais ameaças de cibersegurança da atualidade, a forma como estas se propagam, as principais soluções técnicas existentes e suas funções. Os comportamentos e atitudes que devem ser adotados pelos alunos como forma a prevenir e combater as ameaças de cibersegurança em todas as suas vertentes, foram aqui consideradas.

O objetivo principal destes planos é encorajar a discussão sobre cibersegurança e contribuir para a consciencialização dos riscos. Mas também, contribuir para o desenvolvimento da capacidade de observação, tornando os alunos capazes de distinguir situações de risco e principalmente conhecer comportamentos e atitudes corretos de prevenção e combate a incidentes. O plano encontra-se disponível no anexo C.2.

3.5 QUESTIONÁRIO DE AUTO-DIAGNÓSTICO

Considerando o objetivo do questionário de auto-diagnóstico e, tendo em conta que se decidiu organizar e classificar as perguntas com base na taxonomia de referência de incidentes de segurança utilizada pela rede nacional de CSIRT, o número de perguntas resultante é elevado.

Tormou-se, por isso, necessário definir uma estratégia de seleção de perguntas a incluir no questionário a apresentar aos alunos, evitando que o mesmo fosse demasiado extenso.

Assim, cada vez que um aluno inicia um questionário, são selecionadas de forma aleatória 10 perguntas, uma por cada área de classificação de incidentes.

O feedback, é disponibilizado no final do preenchimento do questionário e é quantitativo, variando entre 0 e 10 pontos e simultaneamente qualitativo, pois apresenta

em caso de resposta incorrecta ou parcialmente correta, informação que pretende levar o aluno a questionar as suas respostas e alterar os seus comportamentos.

Considerando a familiaridade dos alunos com escalas de avaliação e a necessidade de escolher uma escala que apresente um resultado suficientemente representativo do seu desempenho, optou-se por um sistema de classificação incremental onde a pontuação máxima possível é 10. Cada resposta certa atribui 1 ponto, as respostas parcialmente corretas e as respostas erradas podem ter um peso variável, tendo em conta a resposta escolhida, sendo que neste caso, deve ser sempre apresentado feedback de esclarecimento sobre a prática mais segura a adotar e eventual literatura relacionada.

Importa ainda referir que, de cada vez que é feito um acesso ao questionário, é selecionado um novo conjunto de perguntas, o que torna possível que um aluno, ao aceder várias vezes ao questionário, tenha de responder a perguntas distintas, mas sempre com uma pergunta por cada área de classificação de incidentes.

Uma vez criada a lista de perguntas, estas são disponibilizadas aos alunos até que estes terminem de responder sem tempo limite de resposta.

O questionário criado, embora contenha perguntas que abrangem todas as áreas identificadas pela taxonomia, não pode ser considerado como completo. Deve por isso ser melhorado, adicionando e reformulando perguntas para refletir ameaças emergentes e melhorar as perguntas existentes.

O registo das respostas dadas no questionário é feito, e pode ser útil na avaliação do nível de ciberconsciencialização na instituição, dando informação sobre as áreas a reforçar, e a melhorar. O questionário actual encontra-se disponível para consulta no anexo B.2.

3.6 RESUMO DO TRABALHO REALIZADO

Este trabalho pretende que as escolas possam definir uma estratégia de ciberconsciencialização para os alunos, promovendo a utilização eficiente, racional e segura da Internet. A correta definição das estratégias de formação implica uma caraterização da comunidade escolar sobre os conhecimentos gerais de cibersegurança e comportamentos e atitudes adotados pelos alunos e docentes. Este trabalho propõe um modelo representado pela Figura 5 para a construção da ciberconsciencialização em contexto escolar.

Figura 5: Construção da ciberconsciencialização

Trata-se de um processo contínuo que cruza três dimensões fundamentais: avaliação, autodiagnóstico de competências e estratégias de ensino-aprendizagem.

A estratégia de formação deste trabalho procura integrar estas dimensões com três ações complementares para potenciar a ciberconsciência em ambiente escolar:

- questionários entregues aos alunos para avaliar as atitudes e comportamentos de risco;
- questionário de autodiagnóstico para avaliar e melhorar o nível de conhecimento dos alunos em cibersegurança;
- plano de aula a ser integrado na disciplina de TIC e/ou Educação para a Cidadania, para consciencializar os alunos sobre atitudes e comportamentos de segurança cibernética.

A avaliação contínua resulta daobservação de atitudes, comportamentos e habilidades técnicas, enquanto que a aprendizagem contínua é o resultado da interiorização de aprendizagem em sala de aula.

4

ANÁLISE DE RESULTADOS

Este capítulo apresenta os resultados obtidos com a aplicação dos questionários CsA-S e CsB-S.

Os dados foram analisados considerando comportamentos positivos (foi considerado comportamento positivo para classificações iguais ou inferiores a 3 pontos da escala Likert) e atitudes positivas (foi considerada atitude positiva para classificações iguais ou superiores a 4 pontos da escala Likert).

A classificação global da escala CsB-S varia entre 20 e 140 pontos onde uma pontuação mais alta na escala é indicador de comportamentos de segurança cibernética mais arriscados.

Na escala CsA-S, a pontuação varia entre 25 a 100 pontos, sendo uma pontuação alta evidencia de um maior envolvimento na cibersegurança e uma pontuação mais baixa uma atitude negativa e um envolvimento mais baixo.

4.1 CARACTERIZAÇÃO DA POPULAÇÃO ALVO

Os questionários foram disponibilizados na plataforma digital Limesurvey ao público alvo (alunos do 6.º e 9.º ano), tendo o processo de recolha sido realizado durante as aulas de TIC em regime presencial entre 01/04/2021 e 30/04/2021. Do total de alunos convidados a participar, foi recolhida uma amostra de 164 respostas para o questionário CsA-S e de 161 para o questionário CsB-S, igualmente distribuídos entre os géneros masculino e feminino.

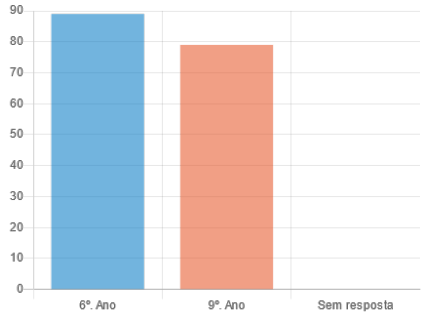
Obtivemos, 88 respostas, provenientes dos alunos de 6.º ano(dos 11 aos 13 anos), cuja média de idades é de 11,76 e 76 respostas, provenientes de alunos de 9.ºano (de 14 a 16 anos) em que a média de idades é 14.73.

4.2 RESUMO POR ITEM DA ESCALA CSA-S

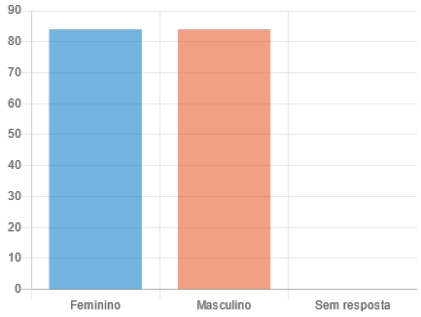
Passo a apresentar as contribuições/respostas por item dos alunos inquiridos no questionário CsA-S, para uma perceção global das atitudes de risco em cibersegurança.

Esta informação foi disponibilizada pela plataforma de publicação e recolha de respostas de questionários LimeSurvey, na secção de estatísticas, apresentando de forma gráfica os dados recolhidos e a sua distribuição pelas opções disponíveis.

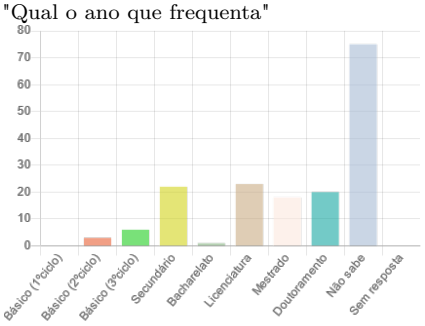
A Figura 6 apresenta os dados de caraterização recolhidos, por género, ano escolar frequentado e habilitações académicas do pai e da mãe e as figuras 7, 8, 9 , 10 e 11 apresentam as respostas dadas pelos alunos.



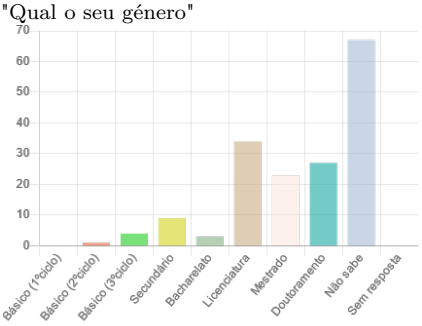
Distribuição de respostas na pergunta "Qual o ano que frequenta"



Distribuição de respostas na pergunta "Qual o seu género"



Distribuição de respostas na pergunta "Habilitações académicas do Pai"

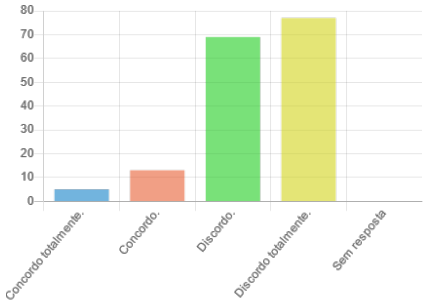


Distribuição de respostas na pergunta "Habilitações académicas da Mãe"

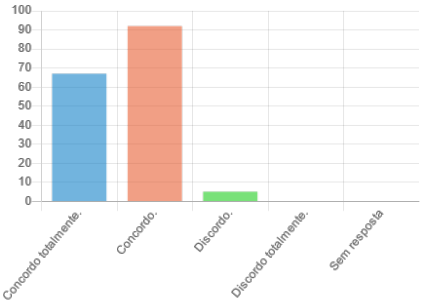
Figura 6: Distribuição dos elementos de caraterização recolhidos no questionário CsA-S

Tendo em conta os dados apresentados na Figura 6, é visível que os 88 participantes (54%) são alunos de 6.º ano e os restantes 76 (46%) alunos de 9.ºano. A distribuição por género é igual tendo 82 inquiridos de cada género. Em relação às habilitações académicas dos pais dos 164 alunos que responderam, 73 (45%) afirmam não saber as habilitações académicas do pai e 66 (40%) não sabem as habilitações da mãe, dos restantes 62 (37%) indicam que o pai tem um grau académico superior e 85 (52%) que o mãe tem um grau académico superior. Dos restantes pais, 8 (5%) têm como

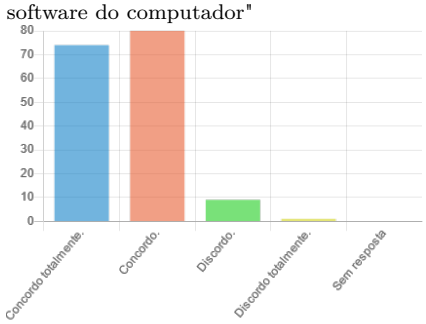
habilitação académica o ensino básico e 21 (13%) o ensino secundário. No caso das mães, 4 (2%) têm como habilitação o ensino básico e 9 (5%), o ensino secundário. Em nenhum dos casos é indicado como habilitação o 1ºciclo do ensino básico.



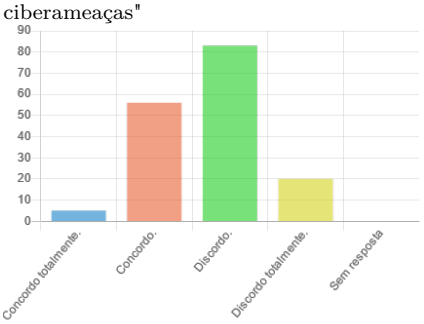
Distribuição de respostas "Acredito que é seguro ignorar avisos de atualizações do software do computador"



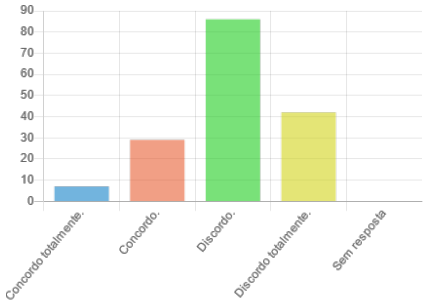
Distribuição de "Estou ciente do meu papel em manter a escola protegida de potenciais ciberameaças"



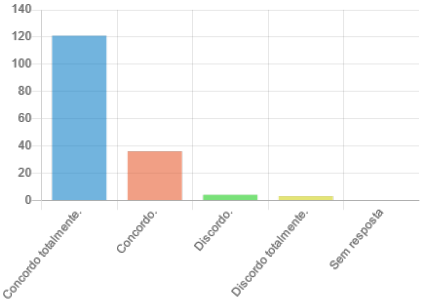
Distribuição de respostas "Penso que todos na escola têm um papel a desempenhar na proteção contra as ciberameaças"



Distribuição de respostas "É difícil saber como posso ajudar a proteger a escola do cibercrime"



Distribuição de respostas "Não tenho as competências necessárias para proteger a escola do cibercrime"



Distribuição de respostas "Acredito que a informação pessoal não deve ser revelada online, nomeadamente quem sou, onde vivo ou que escola frequento"

Figura 7: Distribuição de respostas no questionário CsA-S por pergunta - 1

A figura 7 apresenta as respostas recolhidas nas 6 primeiras perguntas do questionário CsA-S. Na primeira pergunta, *"Acredito que é seguro ignorar avisos de atualizações do software do computador"*, das 164 respostas, 18 concordam totalmente ou concordam, o que indicia uma atitude negativa em 11% das respostas e em 89% uma atitude positiva.

Na pergunta *"Estou ciente do meu papel em manter a escola protegida de potenciais ciberameaças"*, 97% dos alunos concorda ou concorda totalmente, o que revela que os alunos têm consciência da influência das suas atitudes na proteção da escola.

Analisando as respostas à pergunta *"Penso que todos na escola têm um papel a desempenhar na proteção contra as ciberameaças"*, 93% concorda ou concorda totalmente e 6% discorda ou discorda totalmente, o que demonstra que a esmagadora maioria dos alunos acredita que tem um papel a desempenhar para garantir a segurança na escola.

Na pergunta *"É difícil saber como posso ajudar a proteger a escola do cibercrime"*, 37% dos inquiridos concorda ou concorda totalmente com a afirmação enquanto que 63% discorda ou discorda totalmente, evidenciando, que não estão seguros nos comportamentos a adotar, o que aponta para a necessidade de formação e sensibilização sobre atitudes corretas a adotar.

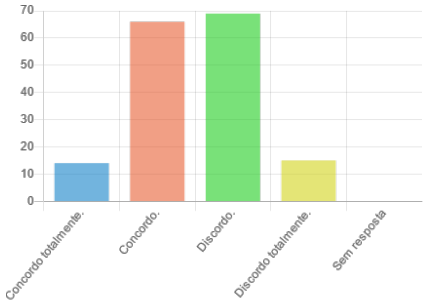
Analisando as respostas dadas na pergunta *"Não tenho as competências necessárias para proteger a escola do cibercrime"*, 22% concorda ou concorda totalmente e 78% discorda ou discorda totalmente, indicando que a maioria dos alunos compreende que as suas atitudes têm influência na segurança da escola e pensa que sabe que atitudes tomar.

Na pergunta *"Acredito que a informação pessoal não deve ser revelada online, nomeadamente quem sou, onde vivo ou que escola frequento"*, 96% concorda ou concorda totalmente e 4% discorda ou discorda totalmente, o que mostra que têm consciência que a divulgação de informação online pode colocar a sua segurança em risco.

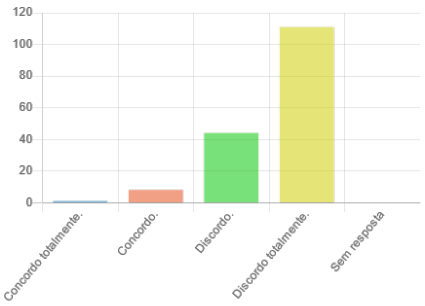
A figura 8 apresenta as respostas recolhidas nas perguntas 7 a 12 do questionário CsA-S.

Na pergunta *"Os sistemas informáticos oferecem toda a proteção de que uma escola necessita"*, 49% concorda ou concorda totalmente e 51% discorda ou discorda totalmente, o que indicia que aproximadamente metade (49%) dos alunos tem uma confiança excessiva na proteção oferecida pelos sistemas informáticos não dando a devida importância às suas atitudes e comportamentos, expondo-os a diversas ameaças como os ataques de Phishing.

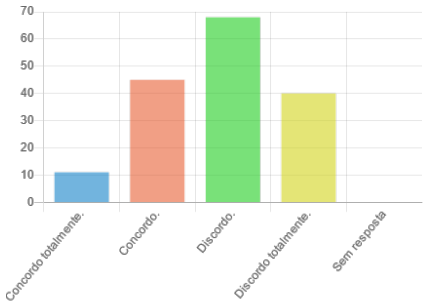
Na segunda pergunta, temos *"Creio que denunciar o cibercrime é uma perda de tempo"*, onde 5% concorda ou concorda totalmente e 95% discorda ou discorda totalmente, o que indicia que os alunos compreendem a importância de denunciar



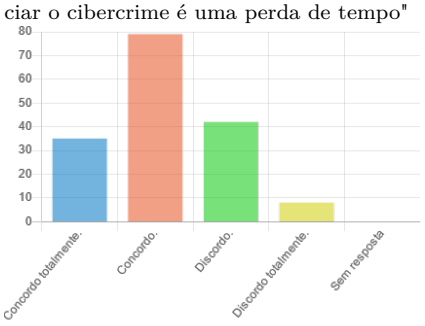
Distribuição de respostas "Os sistemas informáticos oferecem toda a proteção de que uma escola necessita"



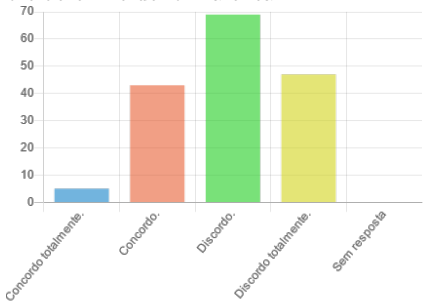
Distribuição de respostas "Creio que denunciar o cibercrime é uma perda de tempo"



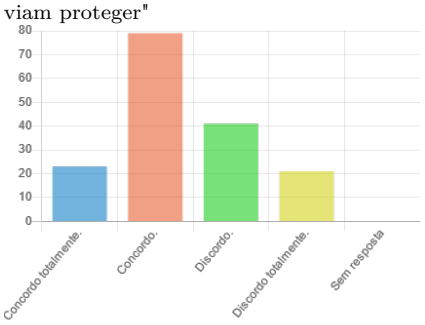
Distribuição de respostas "As autoridades de segurança não tem meios para combater o cibercrime de forma eficaz"



Distribuição de respostas "Creio que os cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger"



Distribuição de respostas "Faria o download de material abrangido por direitos de autor (imagens, documentos, vídeo)"



Distribuição de respostas "Acredito que, quando visualizo conteúdos relacionados com violência em contexto escola"

Figura 8: Distribuição de respostas no questionário CsA-S por pergunta - 2

os ciberataques, contribuindo para a identificação dos cibercriminosos e para a sensibilização e prevenção de novos ataques.

Analisando as respostas dadas na pergunta *"As autoridades de segurança não tem meios para combater o cibercrime de forma eficaz"*, 34% concorda ou concorda totalmente e 66% discorda ou discorda totalmente, o que sugere que aproximadamente um terço dos alunos acha que as autoridades não dispõem dos meios necessários para combater o cibercrime, o que pode representar um problema e funcionar como fator contra a realização da denúncia.

Na pergunta *"Creio que os cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam protege"*, 70% dos alunos concorda ou concorda totalmente e 30% discorda ou discorda totalmente, levando a crer que a maioria não acredita ou acredita pouco nas competências de quem os deve proteger.

Na pergunta *"Faria o download de material abrangido por direitos de autor (imagens, documentos, vídeos)"*, 29% dos alunos concorda ou concorda totalmente e 71% discorda ou discorda totalmente, o que demonstra que aproximadamente um terço dos alunos desconhece que se trata de um crime ou acredita que não terá consequências.

Analisando as respostas dadas na pergunta *"Acredito que, quando visualizo conteúdos relacionados com violência em contexto escolar, posso estar a promover a sua partilha e comentários"*, 62% dos alunos concorda ou concorda totalmente e 38% discorda ou discorda totalmente, o que expressa a existência de um elevado número de alunos (38%) que não compreende totalmente o que é cyberbullying mas também como funcionam os mecanismos de promoção e divulgação online e as consequências da sua promoção e partilha. Indicia que existe um trabalho que ainda pode ser feito em contexto escolar para minimizar/erradicar esta problemática.

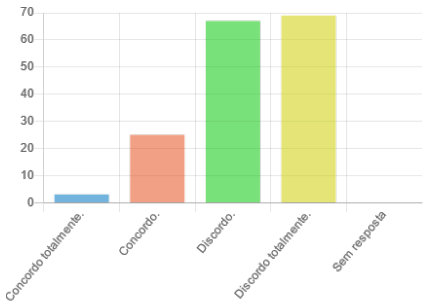
A figura 9 apresenta as respostas recolhidas nas perguntas 13 a 18 do questionário CsA-S.

Analisando as respostas à pergunta *"Receio que, se denunciar um ciberataque às autoridades, isso vá prejudicar a reputação da escola"*, 17% concorda ou concorda totalmente com a afirmação e 83% discorda ou discorda totalmente o que revela que é opinião da esmagadora maioria que a denúncia não prejudica a instituição.

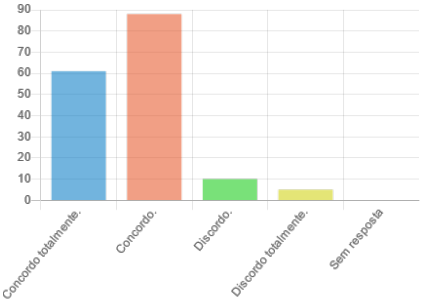
Na pergunta *"Penso que poderá ser feito mais para dar a conhecer/divulgar /sensibilizar os riscos do cibercrime à comunidade educativa"*, 90% enquadra-se na resposta concorda ou concorda totalmente e os restantes 10% discorda ou discorda totalmente o que aponta para que a esmagadora maioria pensa que pode ser feito mais na instituição para divulgar/sensibilizar sobre os riscos de cibersegurança na instituição.

Na pergunta *"Estou a par das regras de utilização dos recursos informáticos da Escola e tento segui-la"*, 93% enquadra-se na resposta concorda ou concorda totalmente e 7% discorda ou discorda totalmente, o que indicia que os alunos têm conhecimento das regras definidas e que tentam segui-las.

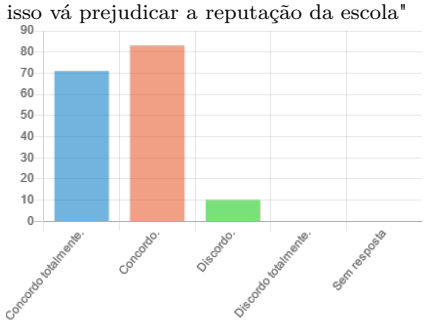
Na pergunta *"Se ocorrer um ciberataque, não sei/não saberei como denunciá-lo"*, 27% enquadram-se na resposta concorda ou concorda totalmente e 73% discorda



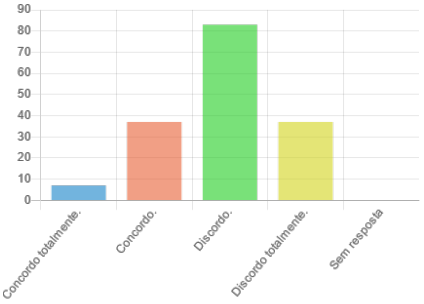
Distribuição de respostas "Receio que, se denúnciar um ciberataque às autoridades, isso vá prejudicar a reputação da escola"



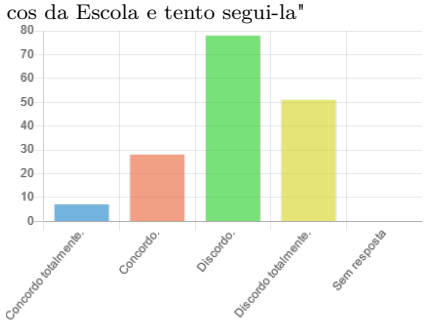
Distribuição de respostas "Penso que poderá ser feito mais para dar a conhecer/divulgar/sensibilizar os riscos do cibercrime à comunidade educativa"



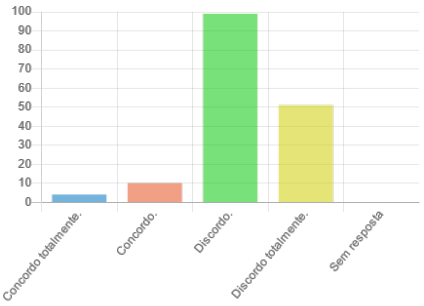
Distribuição de respostas "Estou a par das regras de utilização dos recursos informáticos da Escola e tento segui-la"



Distribuição de respostas "Se ocorrer um ciberataque, não sei/não saberei como denunciá-lo"



Distribuição de respostas "Não acho que seja minha responsabilidade denúnciar um ciberataque que tenha sido lançado a partir da Escola"

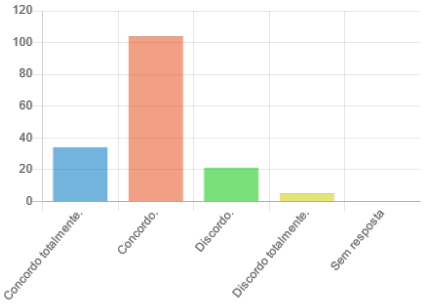


Distribuição de respostas "Não presto atenção à informação disponibilizado pela Escola sobre as ameaças do cibercrime"

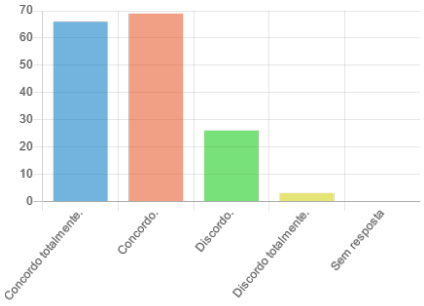
Figura 9: Distribuição de respostas no questionário CsA-S por pergunta - 3

ou discorda totalmente o que indicia que a maioria saberia o que fazer, no entanto quase um terço dos alunos afirma que não saberia o que fazer.

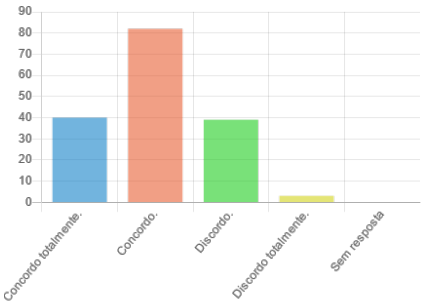
Na pergunta *"Não acho que seja minha responsabilidade denunciar um ciberataque que tenha sido lançado a partir da Escola"*, 21% concorda ou concorda totalmente com a afirmação e 79% discorda ou discorda totalmente o que denota que têm consciência da denúncia como factor de salvaguarda da segurança e como atitude cívica responsável.



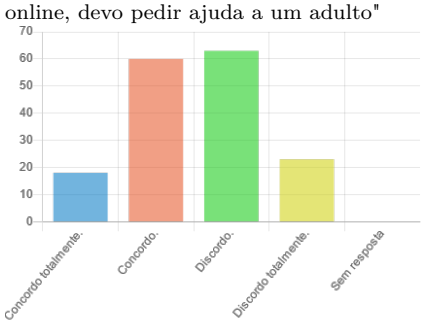
Distribuição de respostas "Confio na minha capacidade de detetaridentificar sinais de um ciberataque"



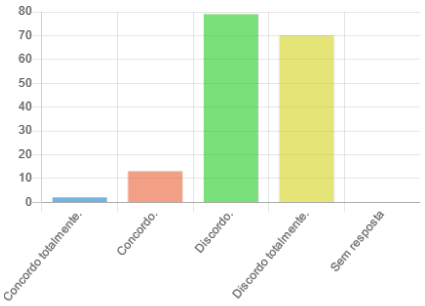
Distribuição de respostas "Acredito que quando aparecem conteúdos inapropriados online, devo pedir ajuda a um adulto"



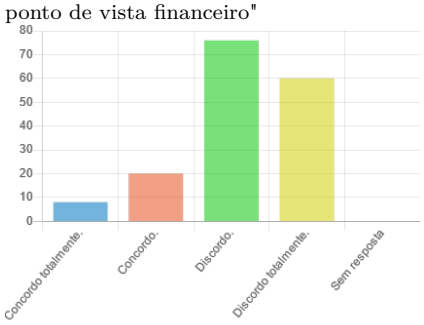
Distribuição de respostas "Sinto que qualquer pessoa da escola está em risco de manipulação por ciber 'vigaristas e burlões'"



Distribuição de respostas "Penso que os cibercriminosos e hackers apenas atingem uma escola quando têm muito a ganhar do ponto de vista financeiro"



Distribuição de respostas "Apenas as grandes empresas e organizações são alvo dos hackers e cibercriminosos"



Distribuição de respostas "Acredito que apenas as instituições que utilizam meios de pagamento online estão em risco de serem vítimas de um ciberataque"

Figura 10: Distribuição de respostas no questionário CsA-S por pergunta - 4

Na pergunta *"Não presto atenção à informação disponibilizado pela Escola sobre as ameaças do cibercrime"* 9% enquadra-se na resposta concorda ou concorda totalmente e 91% discorda ou discorda totalmente, o que aponta que as ações realizadas tiveram impacto nos estudantes tendo conseguido a atenção de maioria dos alunos facilitando a transmissão da mensagem.

A figura 10 apresenta as respostas recolhidas nas perguntas 19 a 24 do questionário CsA-S.

Analisando as respostas dadas na pergunta *"Confio na minha capacidade de detetar/identificar sinais de um ciberataque"*, 63% concorda, 21% concorda totalmente e 16% discorda ou discorda totalmente, o que indica que 84% acredita ser capaz de identificar os sinais de um ciberatques.

Na pergunta *"Acredito que quando aparecem conteúdos inapropriados online, devo pedir ajuda a um adulto"*, as respostas estão distribuídas da seguinte forma: 82% concorda ou concorda totalmente e 18% discorda ou discorda totalmente, indiciando que uma grande maioria dos alunos quando se depara com algo estranho, incómodo ou perturbador pense que o conteudo não é adequado para eles são capazes de pedir ajuda a um adulto.

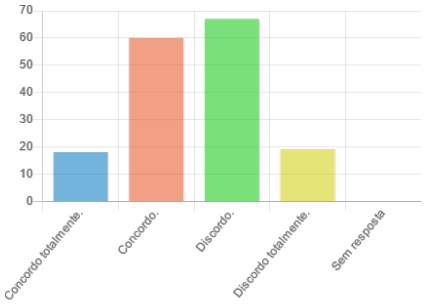
Analisando as respostas dadas na pergunta *"Sinto que qualquer pessoa da escola está em risco de manipulação por ciber "vigaristas e burlões*, 74% concorda ou concorda totalmente e 26% discorda ou discorda totalmente, o que evidencia que os alunos estão conscientes da existência de pessoas mal intencionadas online que se tentam aproveitar de outras pessoas, recorrendo a uma grande diversidade de esquemas. Os alunos, estando atentos a esta realidade, tomam consciência que todos podem ser vitimas, sendo isto um passo importante para garantir a sua proteção online.

Na pergunta *"Penso que os cibercriminosos e hackers apenas atingem uma escola quando têm muito a ganhar do ponto de vista financeiro"*, as respostas estão distribuídas da seguinte forma, 48% concorda ou concorda totalmente e 52% discorda ou discorda totalmente demonstrando que, aproximadamente, metade os alunos têm dúvidas sobre as motivações e objetivos dos atacantes.

Analisando as respostas dadas na pergunta *"Apenas as grandes empresas e organizações são alvo dos hackers e cibercriminosos"*, 9% concorda ou concorda totalmente e 91% discorda ou discorda totalmente, o que indica que os alunos compreendem que todos podem ser alvo de ataque por cibercriminosos.

Na pergunta *"Acredito que apenas as instituições que utilizam meios de pagamento online estão em risco de serem vítimas de um ciberataque"*, as respostas estão distribuídas da seguinte forma: 17% concorda ou concorda totalmente e 82% discorda ou discorda totalmente, o que aponta para que os alunos têm consciência que todas as instituições e pessoas individuais podem ser vitimas de ciberataques, dai a importância de estarem preparados para fazer face a esta realidade.

A figura 11 apresenta as respostas recolhidas na pergunta 25 do questionário CsA-S.



Distribuição de respostas "Penso que tenho o direito de estar sempre online, com acesso a todos os serviços da Internet"

Figura 11: Distribuição de respostas no questionário CsA-S - 5

Analisando as respostas dadas na pergunta *"Penso que tenho o direito de estar sempre online, com acesso a todos os serviços da Internet"*, 48% concorda ou concorda totalmente e 52% discorda ou discorda totalmente, indiciando que aproximadamente, metade dos inquiridos pode estar a desenvolver dependência da ligação à Internet e dos seus serviços.

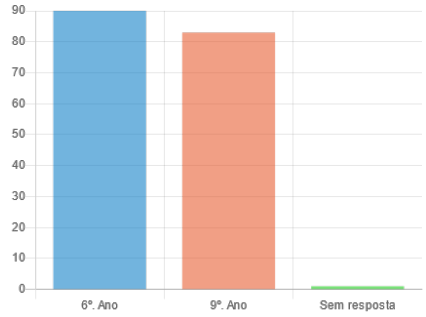
4.3 RESUMO POR ITEM DA ESCALA CSB-S

No questionário CsB-S são avaliados os comportamentos dos alunos. Este questionário é composto, tal como o anterior, de perguntas de caraterização dos alunos e perguntas de avaliação dos comportamentos. De seguida, vão ser apresentados os dados recolhidos, na forma de gráficos, com o intuito de disponibilizar uma perceção global.

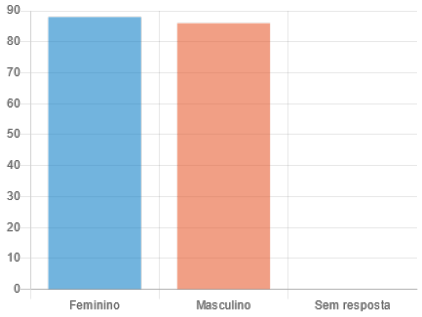
Tendo em conta que o questionário foi disponibilizado na plataforma de publicação e recolha de respostas de questionários LimeSurvey, é possivel extrair uma representação gráfica dos dados recolhidos com a sua distribuição pelas opções selecionadas pelos alunos.

Assim a figura 12 apresenta os dados de caraterização recolhidos, por género, ano escolar frequentado e habilitações académicas do pai e da mãe e as figuras 13, 14, 15 e 16 apresentam as respostas dadas pelos alunos.

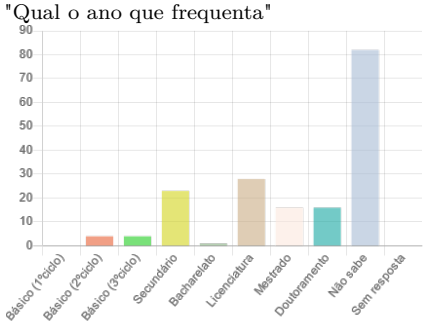
Analisando os dados de caraterização recolhidos com o questionários CsB-S, é visível que 52% (84) dos participantes são alunos de 6.º ano e os restantes 48% (76) correspondem a alunos de 9.ºano. No que diz respeito à distribuição por género é 81 inquiridos são do género feminino o que corresponde a 51% e 79 são do género masculino o que corresponde a 49% dos inquiridos. Em termo de habilitações



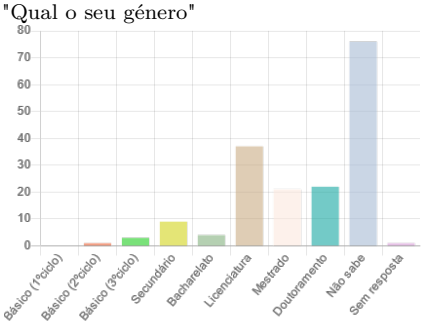
Distribuição de respostas na pergunta "Qual o ano que frequenta"



Distribuição de respostas na pergunta "Qual o seu género"



Distribuição de respostas na pergunta "Habilitações académicas do Pai"



Distribuição de respostas na pergunta "Habilitações académicas da Mãe"

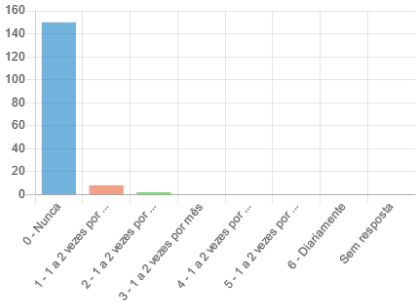
Figura 12: Distribuição dos elementos de caraterização recolhidos no questionário CsB-S

académicas dos pais dos 161 alunos inquiridos no questionário CsB-S, 73 (46%) afirma não saber as habilitações académicas do pai e 67 (42%) não sabem as habilitações da mãe, dos restantes 56 (38%) indicam que o pai tem um grau académico superior e 80 (50%) que o mãe tem um grau académico superior. Dos restantes, 8 (5%) dos pais têm como habilitação académica, o ensino básico e 21 (13%) o ensino secundário. No caso das mães 4 (3%) têm o ensino básico e 9 (6%) o ensino secundário. Em nenhum dos casos é indicado como habilitação o 1ºciclo do ensino básico.

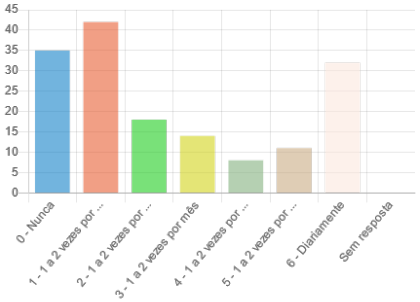
A distribuição de respostas nas perguntas 1 a 6 do questionário CsB-S são apresentada na figuras 13.

Analisando as respostas à pergunta *"Partilhar palavras-passe com colegas"*, 94% afirma que nunca partilha palavras-passe, 5% que partilha de 1 a 2 vezes por semestre e 1% de 1 a 2 vezes por trimestre, indiciando que a esmagadora maioria dos alunos não partilha as suas palavras passe. No entanto existe uma minoria de cerca de 6% que o faz.

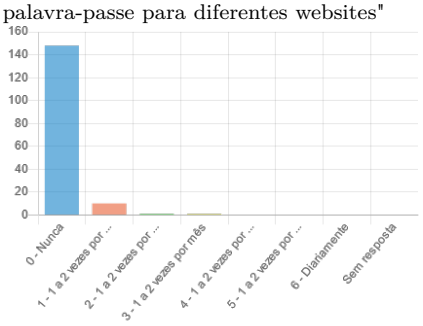
Analisando as respostas à pergunta *"Usar ou criar palavras-passe demasiado simples (ex.: nome de familiar, data de nascimento, apelidos, sequências de carateres)"*, apenas 63% afirma que nunca usa ou cria palavras-passe simples, 24% afirma que utiliza 1 a 2 vezes por semestre, 6% utiliza 1 a 2 vezes por trimestre e 3% entre 1 a



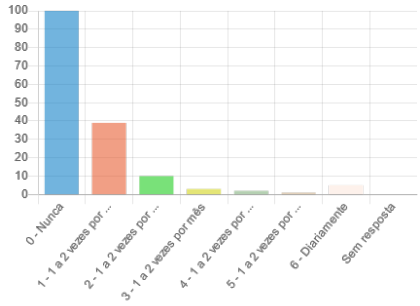
Distribuição de respostas "Partilhar palavras-passe com colegas"



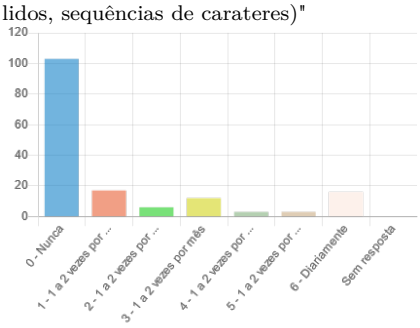
Distribuição de respostas "Usar a mesma palavra-passe para diferentes websites"



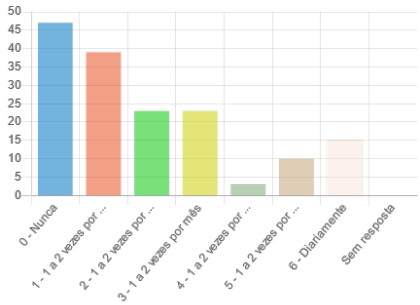
Distribuição de respostas "Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita"



Distribuição de respostas "Usar ou criar palavras-passe demasiado simples (ex.: nome de familiar, data de nascimento, apelidos, sequências de carateres)"



Distribuição de respostas "Usar sistemas de armazenamento online (cloud) para partilhar ou guardar informação pessoal e sensível"



Distribuição de respostas "Usar redes Wi-Fi de acesso livre (públicas)"

Figura 13: Distribuição de respostas no questionário CsB-S por pergunta - 1

2 vezes por mês e 1 a 2 vezes por semana e 3% utiliza diariamente. Assim pode-se concluir que 37% dos alunos continua a utilizar palavras-passe demasiado simples, o que representa um elevado risco pare eles e para a escola, sendo por isso uma das áreas de risco e que necessita de ser trabalhada.

Na pergunta *"Usar a mesma palavra-passe para diferentes websites"*, 22% afirma que nunca usa a mesma palavra-passe, 26% utiliza 1 a 2 vezes por trimestre, 32% de 1 a 2 vezes por mês a 1 a 2 vezes por semana e 20% afirma que o faz diariamente. A utilização da mesma palavra-passe em vários website é uma prática que compromete gravemente a segurança dos utilizadores e das instituições onde eles estão inseridos.

Considerando que é uma prática utilizada com maior ou menor frequência por 74% dos inquiridos, trata-se de uma área de risco que necessita de ser trabalhada em contexto escolar.

Na pergunta *"Usar sistemas de armazenamento online (cloud) para partilhar ou guardar informação pessoal e sensível"*, a distribuição das respostas indica que 64% nunca utiliza o armazenamento online, 25% utiliza entre 1 a 2 vezes por semestre a 1 a 2 vezes por semana e 10% utiliza diariamente. Considerando que 26% utiliza este sistema de armazenamento de informação, é importante alertar os alunos para os riscos envolvidos e dar-lhes a conhecer as opções de segurança que podem adoptar para minimizar os riscos.

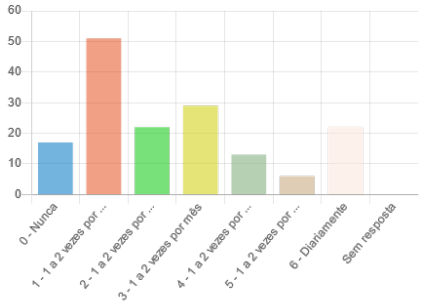
Analisando as respostas à pergunta *"Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita"*, 83% afirma que nunca o faz e 10% afirma que o faz 1 a 2 vezes por semestre e 1% de 1 a 2 vezes por trimestre a 1 a 2 vezes por mês. Considerando que a inserção de dados de pagamento sem a informação/certificação de segurança explícita representa um grave risco de segurança e o possivel impacto na vida dos alunos e das suas familias, embora sejam apenas 17% dos inquiridos a fazê-lo, será importante a seu inclusão em ações de sensibilização.

Analisando as respostas à pergunta *"Usar redes Wi-Fi de acesso livre (públicas)"*, 29% afirma que nunca utiliza e os restantes 71% utiliza entre 1 a 2 vezes por semestre a diariamente. Considerando que este tipo de redes são utilizadas por um conjunto de desconhecidos de quem pouco ou nada se sabe é, extremamente importante, alertar os alunos para os perigos da sua utilização bem como sobre os procedimentos para minimizar o risco em caso de necessidade da sua utilização.

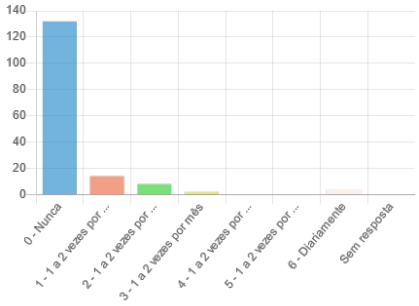
A distribuição de respostas nas perguntas 7 a 12 do questionário CsB-S são apresentadas na figuras 14.

Na pergunta *"Confiar nos conselhos de um amigo ou colega próximo sobre aspetos de segurança online"*, apenas 10% afirma que não recorre a conselhos de colegas ou amigos, 32% recorre 1 a 2 vezes por semestre, e 14% afirma recorrer 1 a 2 vezes por trimestre, 18% recorre 1 a 2 vezes por mês e 25% afirma recorrer mais de 1 vez por quinzena. As respostas recolhidas nesta pergunta demonstram que 68% dos alunos se sentem pouco seguros a reagir às ocorrências online e recorrem a amigos e colegas.

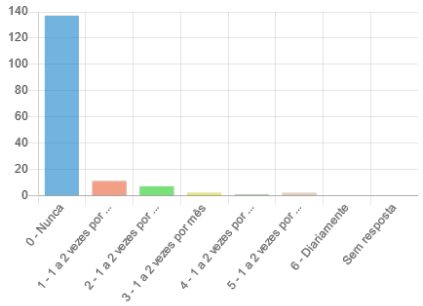
Na pergunta *"Descarregar software/apps antivírus gratuito de fontes desconhecidas"*, 83% diz nunca o fazer, 9% diz fazê-lo 1 a 2 vezes por semestre, 5% diz que o faz 1 a 2 vezes por trimestre, 1% que o faz 1 a 2 vezes por mês e 3% diz



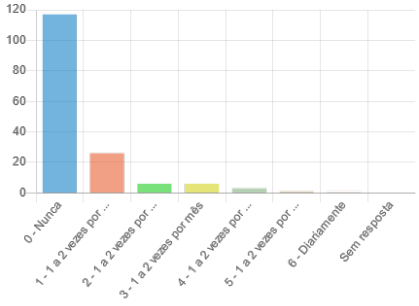
Distribuição de respostas "Confiar nos conselhos de um amigo ou colega próximo sobre aspetos de segurança online"



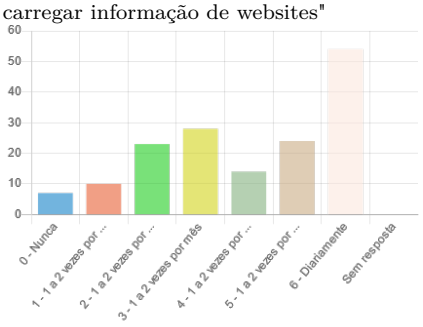
Distribuição de respostas "Descarregar software/apps antivírus gratuito de fontes desconhecidas"



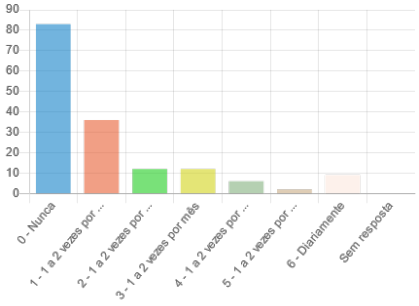
Distribuição de respostas "Desativar o antivírus do computador para que possa descarregar informação de websites"



Distribuição de respostas "Utilizar a pen drive pessoal com a finalidade de transferir informação para os computadores da Escola"



Distribuição de respostas "Verificar regularmente as atualizações de software do smartphone/tablet/portátil/PC"



Distribuição de respostas "Descarregar conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas"

Figura 14: Distribuição de respostas no questionário CsB-S por pergunta - 2

fazê-lo diariamente. A transferência de software e/ou apps de fontes desconhecidas representa uma das maiores fontes de problemas nas aplicações, pois muitas vezes incluem código malicioso. Considerando que 17% dos alunos afirma fazê-lo em algum momento esta prática representa um problema de segurança que deve ser abordado.

Analisando as respostas à pergunta *"Desativar o antivírus do computador para que possa descarregar informação de websites"*, 86% afirma nunca o fazer, 7% diz fazê-lo 1 a 2 vezes por semestre, 4% 1 a 2 vezes por trimestre, 3% afirma fazê-lo de 1 a 2 vezes por mês a 1 a 2 vezes por semana. Considerando que o antivirus é um mecanismo de segurança, a sua desativação para aceder a conteúdos online nunca

deve acontecer. Tendo em conta que 14% dos alunos fiz fazê-lo indicia que estão a colocar a segurança em risco.

Analisando as respostas à pergunta *"Utilizar a pen drive pessoal com a finalidade de transferir informação para os computadores da Escola"*, 73% diz nunca o fazer, 16% utiliza 1 a 2 vezes por semestre e 11% distribui as suas respostas entre 1 a 2 vezes por trimestre e 1 a 2 vezes por semana. Assim, 27% assume utilizar dispositivos amovíveis para transferir informação de e para os computadores, o que representa um problema de segurança e de privacidade que deve ser tratado.

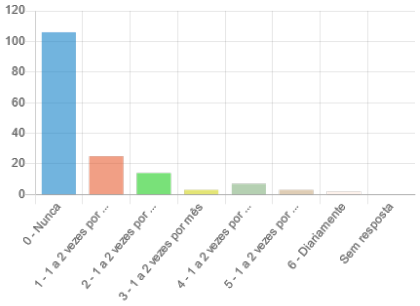
Na pergunta *"Verificar regularmente as atualizações de software do smartphone/tablet /portátil/PC"*, 4% diz nunca o fazer, 6% diz fase-lo 1 a 2 vezes por semestre, 14% diz fazê-lo 1 a 2 vezes por trimestre e 18% de 1 a 2 vezes por mês a 1 a 2 vezes por semana e 35% diariamente. Os alunos, na sua esmagadora maioria, cumprem com este comportamento de segurança.

Na pergunta *"Descarregar conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas"*, 52% afirma nunca o fazer, 23% diz fazê-lo 1 a 2 vezes por semestre 8% diz fazê-lo 1 a 2 vezes por trimestre, 8% diz fazê-lo 1 a 2 vezes por mês e 11% diz fazê-lo entre 1 a 2 vezes por quinzena a diariamente. Este comportamento indicia um desrespeito pelos direitos de autor e uma tendência de apoio à pirataria que tem de ser combatida.

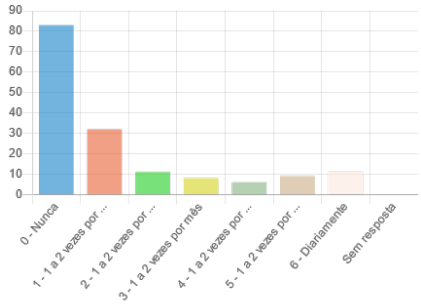
A distribuição de respostas nas perguntas 13 a 18 do questionário CsB-S é apresentada na figuras 15.

Analisando as respostas à pergunta *"Partilhar a sua localização nas redes sociais (Fotos, local de férias...)"*, 66% diz nunca partilhar, 16% partilha 1 a 2 vezes por semestre, 9% partilha 1 a 2 vezes por trimestre e 9% partilha de 1 a 2 vezes por mês a diariamente. Considerando que 34% dos alunos assume em algum momento ter partilhado informação privada e a sua localização, estes estão a colocar em causa a sua segurança e dos seus bens, sendo por isso necessária uma intervenção nesta área.

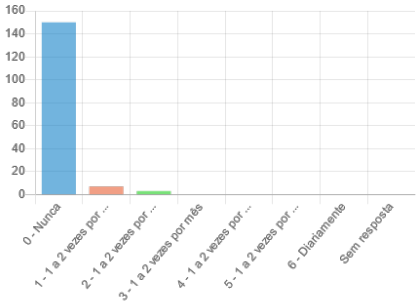
Na pergunta *"Aceitar pedidos de amizade em redes sociais porque reconhece fotos"*, 52% dos alunos afirma nunca o fazer, 20% afirma fazê-lo 1 a 2 vezes por semestre e 28% afirma aceitar de 1 a 2 vezes por trimestre a diariamente. Considerando que a criação de contas falsas em redes sociais e o roubo de identidade são práticas que continuam a ser frequentes online, aceitar pedidos de amizade só por reconhecer a foto coloca em risco a sua segurança e dos seus amigos pelo que não deve ser feito. Analisando as respostas recolhidas cerca de 48% dos alunos não tem esta atitude.



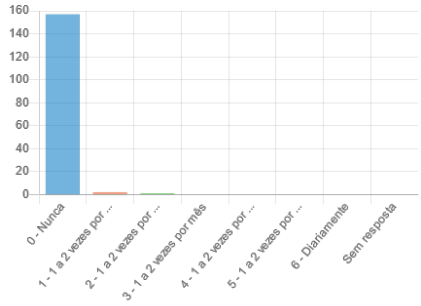
Distribuição de respostas "Partilhar a sua localização nas redes sociais (Fotos, local de férias...)"



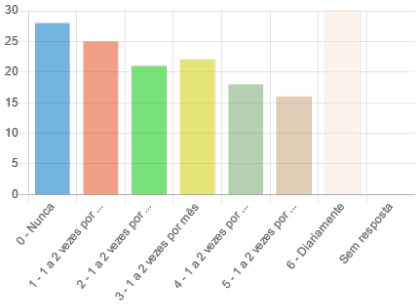
Distribuição de respostas "Aceitar pedidos de amizade em redes sociais porque reconhece fotos"



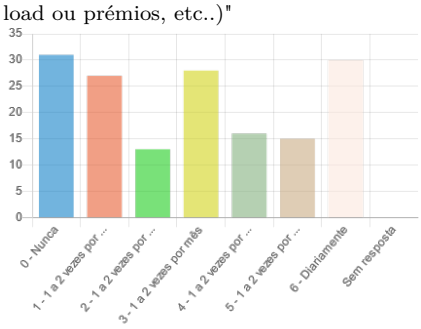
Distribuição de respostas "Clicar em links em emails recebidos de uma fonte desconhecida"



Distribuição de respostas "Enviar informação pessoal a estranhos pela Internet (contactos nas redes sociais, dar números de telefone ou email para obter códigos de download ou prémios, etc..)"



Distribuição de respostas "Clicar em links de email enviados por amigos próximos ou por colegas de Escola"



Distribuição de respostas "Verificar atualizações para quaisquer antivírus que tenha instalado"

Figura 15: Distribuição de respostas no questionário CsB-S por pergunta - 3

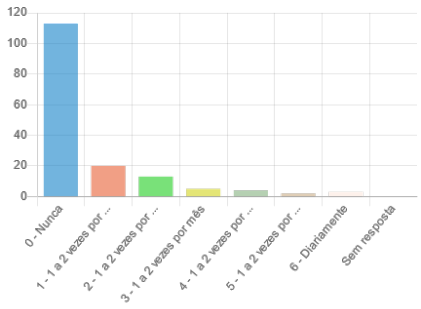
As respostas à pergunta *"Clicar em links em emails recebidos de uma fonte desconhecida."*, 94% afirma não clicar em links de emails de fonte desconhecida e 6% clica entre 1 a 2 vezes por semestre e 1 a 2 vezes por trimestre. Considerando que os links em emails são uma das principais formas de difusão de malware utilizadas nos esquemas de phishing, o simples facto de existirem alunos dispostos a clicar nestes links representa um risco que tem de ser minimizado, com formação.

Analisando as respostas à pergunta *"Enviar informação pessoal a estranhos pela Internet (contactos nas redes sociais, dar números de telefone ou email para obter códigos de download ou prémios, etc..)"*, 98% afirma que que não envia informação

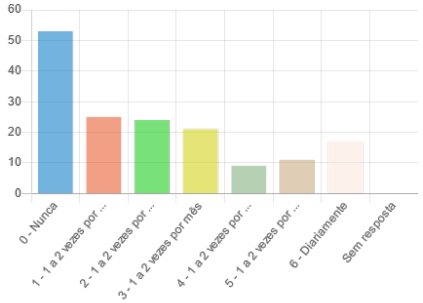
a estranhos, no entanto, 1% diz enviar 1 a 2 vezes por semestre e 1% diz enviar 1 a 2 vezes por trimestre. Sendo a partilha de informação com estranhos um comportamento de alto risco, a esmagadora maioria dos inquiridos(98%) reconhece-o como tal.

Na pergunta *"Clicar em links de email enviados por amigos próximos ou por colegas de Escola"*, 18% respondeu nunca, 16% respondeu 1 a 2 vezes por semestre, 13% respondeu 1 a 2 vezes por trimestre, 14% respondeu 1 a 2 vezes por mês, 11% respondeu 1 a 2 vezes por quinzena, 10% 1 a 2 vezes por semana e 19% deu a resposta diariamente. Estes resultados indiciam um comportamento positivo ao clicarem apenas em links provenientes de pessoas de confiança.

As respostas à pergunta *"Verificar atualizações para quaisquer antivírus que tenha instalado"*, 19% afirma nunca o fazer, 17% diz que o faz 1 a 2 vezes por semestre, 8% diz que o faz 1 a 2 vezes por trimestre, 18% diz que o faz 1 a 2 vezes por mês ,10% diz que o faz 1 a 2 vezes por quinzena, 9% diz que o faz 1 a 2 vezes por semana e 19% diz que o faz diariamente. Considerando o número elevadíssimo de novas ameaças que surgem diariamente, é fundamental garantir que o antivírus esteja atualizado para as detetar. Assim, é urgente melhorar este comportamento dos alunos, incentivando-os e sensibilizando-os para a necessidade de instalação das actualizações de forma frequente e regular.



Distribuição de respostas "Descarregar informação e material de websites para o computador sem verificação da veracidade"



Distribuição de respostas "Guardar informação pessoal, de familiares e amigos no dispositivo eletrónico pessoal (por ex., smartphone/tablet/portátil)"

Figura 16: Distribuição de respostas no questionário CsB-S por pergunta - 4

A distribuição de respostas nas perguntas 19 e 20 do questionário CsB-S é apresentada na figura 16.

Na pergunta *"Descarregar informação e material de websites para o computador sem verificação da veracidade"*, 71% afirma nunca o fazer, e os restantes 29% estão distribuídos entre 1 a 2 vezes por semestre e diariamente. Tendo em conta que 29% dos alunos transfere a informação sem consultar a sua veracidade e que as notícias

e informação falsas são um problema que tem crescido de forma exponencial, é importante continuar a fomentar a análise critica da informação consultada.

Analisando as respostas à pergunta *"Guardar informação pessoal, de familiares e amigos no dispositivo eletrónico pessoal (por ex., smartphone/tablet /portátil)"*, 33% afirma que não o faz, 16% afirma que o faz 1 a 2 vezes por semestre, 15% afirma que o faz 1 a 2 vezes por trimestre, 13% afirma que o faz 1 a 2 vezes por mês, 6% afirma que o faz 1 a 2 vezes por quinzena, 7% afirma que o faz 1 a 2 vezes por semana e 11% diz que o faz diariamente. Considerando que 77% diz guardar informação pessoal, de familiares e amigos no dispositivo eletrónico pessoal, torna-se evidente a necessidade da consciencialização para os riscos deste tipo de prática e o conhecimento das medidas de segurança disponíveis para adoção em caso de necessidade da sua utilização.

Globalmente, é evidente que os alunos têm um conjunto de comportamentos que colocam em risco a sua segurança, a segurança da instituição e a dos seus familiares e amigos, o que justifica a necessidade de ações de sensibilização em contexto escolar.

4.4 DESCOBERTAS IDENTIFICADAS

Esta secção detalha os resultados obtidos com os questionários CsA-S e CsB-S e a análise efetuada para responder às perguntas da investigação.

A tabela 4 apresenta as perguntas da investigação a que os questionários pela análise da informação recolhida permitiram responder e o conjunto de perguntas dos questionários CsA-S e CsB-S utilizadas para justificar as respostas.

A análise de variação das respostas e dados em falta foi feita com recurso estatística descritiva.

Para identificar e eliminar os itens com dados em falta, foi realizada uma análise descritiva individual dos itens, tendo-se obtido uma amostra com 88 alunos de 6.º ano e 76 alunos de 9.º ano.

Na análise foram considerados como comportamentos positivos resultados iguais ou menores que 3 pontos da escala Likert. Nas escala de atitudes foram considerados como positivos resultados iguais ou maiores a 4 pontos da escala Likert.

A classificação global da escala CsB-S varia entre 20 a 140, onde valores baixos indicam comportamento de baixo risco em segurança cibernética e a pontuação global da escala CsA-S varia entre 25 a 100, onde valores altos são indicativos de atitudes de baixo risco.

ID	Pergunta	ID Perguntas questionário
1	Os alunos expressam algum nível de consciência sobre sua privacidade online e as consequências de expor seus dados pessoais?	A6,B5,B13, B14,B16, B20
2	As atitudes e comportamentos online dos alunos são tendencialmente positivos ou negativos?	A11,A12,A17, A25,B8,B9, B12,B19,A8
3	Qual é a percepção dos alunos sobre as informações de segurança cibernética fornecidas pela escola?	A14,A15,A16, A17,A18
4	Ao entrar em contato com estranhos online, os alunos estão cientes das preocupações envolvidas?	B2,B4,B5, B14,B15,B17
5	Os alunos estão cientes da influência das suas atitudes e comportamentos em relação à segurança cibernética na escola?	A1,A2,A3, A4,A5,A7, B2,B9,B11
6	Os alunos entendem as motivações dos cibercriminosos?	A19,A22, A23,A24
7	Os alunos contam com as autoridades de segurança e técnicos de TIC?	A8,A9,A10, A13
8	Os alunos estão cientes de como proteger os seus equipamentos e dados?	B1,B2,B3, B6,B8,B9, B10,B11, B18,B20
9	Os alunos estão conscientes sobre as consequências do uso não oficial de software protegido contra cópia e gravação?	B8,B12,B19

Tabela 4: Perguntas da investigação a que foi possível responder.

Os dados foram analisados de acordo com a estratificação por género e grupos de séries e apresentados como média e proporções. Para comparar as médias das classificações globais entre género e grau foi utilizado um *T-test* para amostras independentes e considerado um nível de significância de 5%.

A análise estatística dos dados foi realizada com o software IBM SPSS (Statistical Package for the Social Sciences, versão 26).

Para além das perguntas apresentadas na tabela 4 foram definidas mais três perguntas da investigação às quais não foi possível obter uma resposta conclusiva. Na tentativa de responder à pergunta *"Existe algum indicador de atitudes e comportamentos que esteja claramente relacionado com o género?"*, utilizou-se o *Rank-biserial correlation coefficients* entre o género e os indicadores de comportamentos(B) e atitudes(A) tendo-se obtido a tabela 5 que apresenta as correlações.

B1	-0.078	B11	-0.080	A1	0.033	A11	-0.030	A21	-0.008
B2	-0.076	B12	0.195	A2	0.067	A12	-0.070	A22	-0.063
B3	0.078	B13	-0.073	A3	-0.089	A13	0.016	A23	-0.082
B4	-0.043	B14	-0.099	A4	0.086	A14	0.043	A24	-0.090
B5	-0.014	B15	0.022	A5	0.196	A15	-0.031	A25	-0.022
B6	-0.007	B16	0.067	A6	-0.010	A16	0.109		
B7	-0.023	B17	0.079	A7	0.086	A17	-0.083		
B8	0.016	B18	-0.138	A8	-0.050	A18	-0.158		
B9	0.147	B19	-0.075	A9	-0.077	A19	0.063		
b10	-0.084	B20	0.016	A10	-0.144	A20	-0.254		

Tabela 5: Coeficientes de correlação *Rank-biserial* entre género e indicadores de comportamento (B) e atitude (A).

Analisando os resultados (apresentados na tabela 5) não foram encontradas correlações de atitudes e comportamentos que estejam claramente relacionados com o género.

As figuras 17 e 18 apresentam graficamente a distribuição de comportamentos por género.

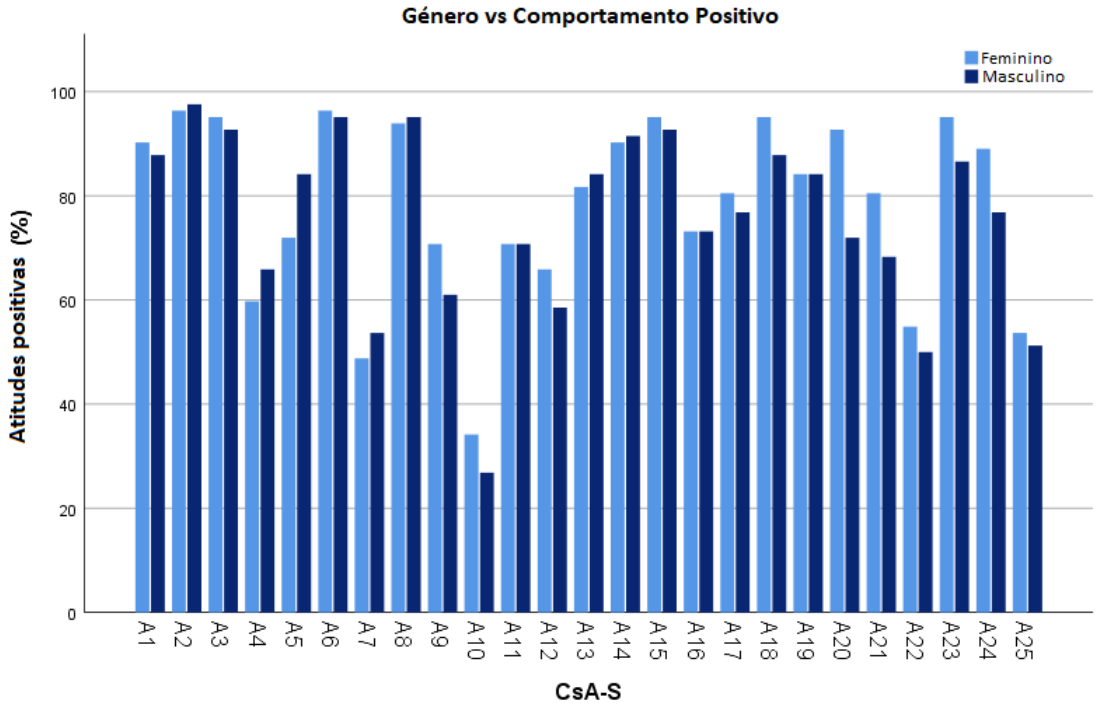


Figura 17: Gênero vs Comportamento Positivo na escala CsB-s

A segunda pergunta à qual não foi possível obter uma resposta conclusiva foi a *"Com base nas respostas é possível identificar uma diferença no nível de consciencialização e capacidade de resposta ao risco com base no ano que frequentam?"*.

Na tentativa de determinar uma resposta foi utilizado o coeficientes de correlação *Kendall´s tau-b* entre o nível de ensino dos alunos e os indicadores de comportamento (B) e atitude (A) tendo-se obtido a tabela de correlação 6.

A distribuição de comportamentos por nível de ensino é apresentada nas figuras 19 e 20.

Na pergunta *"As habilitações académicas dos pais têm associação nos comportamentos de risco dos alunos(filhos)?"* foi aplicada a correlação *Kendal-tau-b* não tendo sido identificadas correlações entre entre as qualificações dos pais e os comportamentos e atitudes dos alunos.

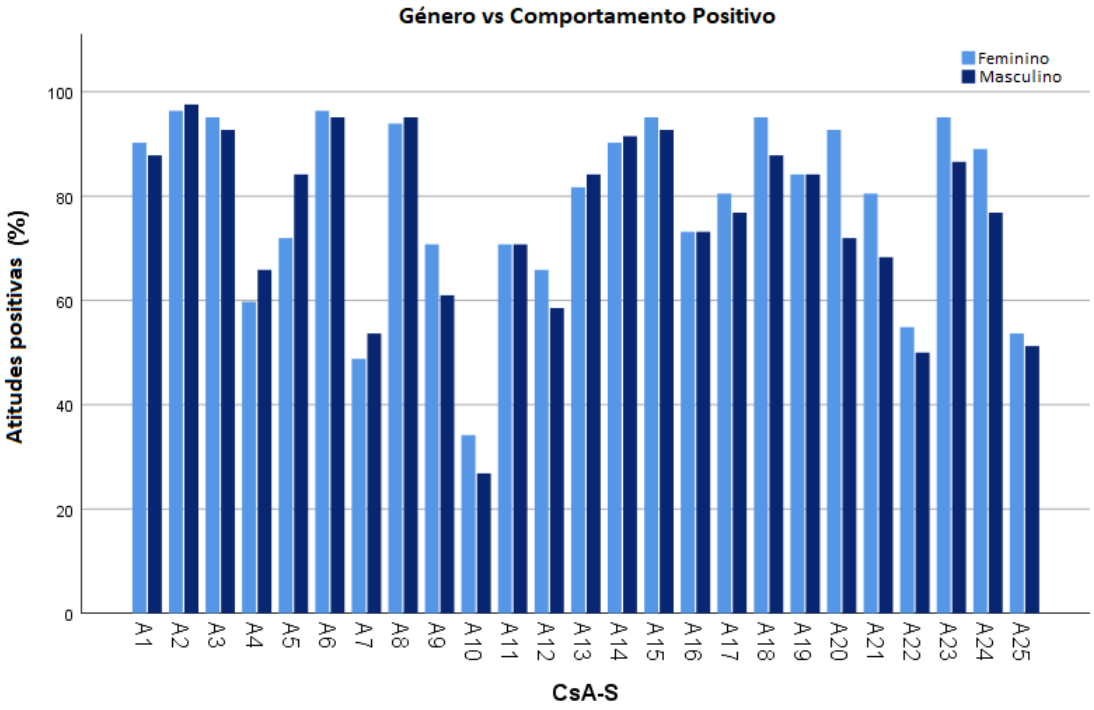


Figura 18: Gênero vs Atitudes Positivas na escala CsA-s

B1	0.111	B11	0.039	A1	-0.194	A11	-0.437	A21	-0.026
B2	0.041	B12	0.174	A2	-0.412	A12	-0.064	A22	-0.064
B3	0.241	B13	0.318	A3	-0.132	A13	-0.344	A23	-0.098
B4	0.162	B14	0.121	A4	-0.020	A14	0.093	A24	-0.088
B5	-0.079	B15	-0.036	A5	-0.177	A15	-0.296	A25	-0.195
B6	0.063	B16	0.054	A6	-0.241	A16	-0.195		
B7	0.107	B17	0.056	A7	0.109	A17	-0.213		
B8	-0.079	B18	0.012	A8	-0.240	A18	-0.360		
B9	0.215	B19	0.160	A9	-0.374	A19	-0.170		
b10	0.084	B20	0.073	A10	-0.195	A20	-0.390		

Tabela 6: Coeficientes de correlação *Kendall´s tau-b* entre o nível de ensino dos alunos e indicadores de comportamento (B) e atitude (A).

Para as restantes perguntas foram encontradas respostas, sendo de seguida apresentadas as conclusões e o processo de análise utilizado.

Em termos de consciencialização sobre privacidade online os alunos demonstram comportamentos positivos (figura 21a) e atitudes positivas (figura 21b), tendo o item B20, relativo ao armazenamento de informações, apresentado o menor comportamento positivo (64%).

Relativamente ao acesso a serviços de Internet os alunos também apresentam comportamentos (figura 22a) e atitudes (figura 22b), tendencialmente, positivos com o menor valor positivo de 52% no resultado 2.

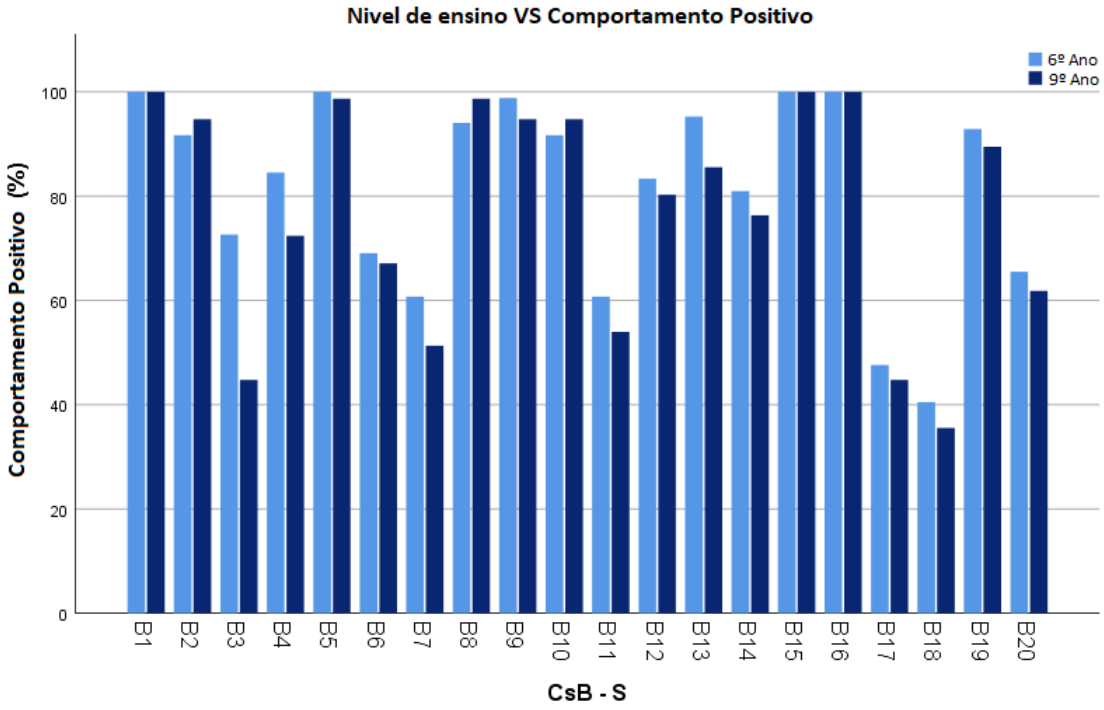


Figura 19: Nível de ensino vs Comportamentos Positivas na escala CsB-s

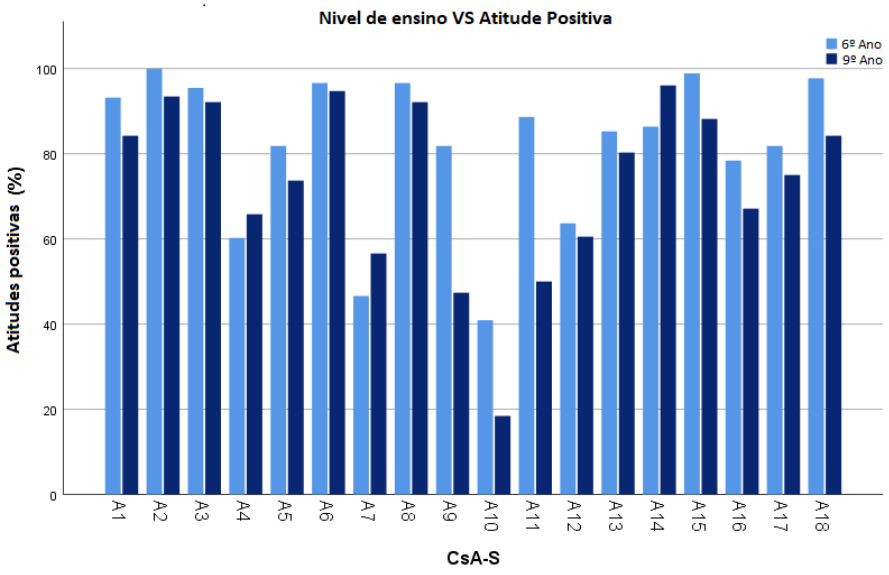
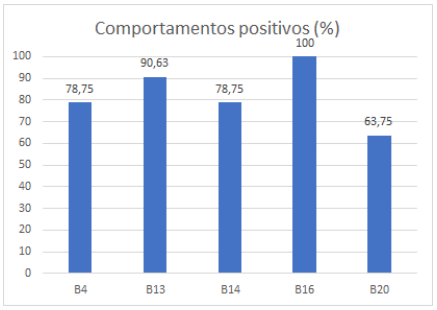
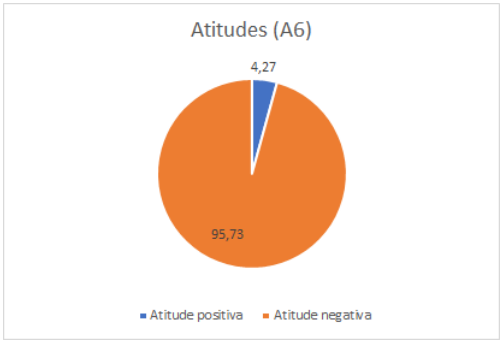


Figura 20: Nível de ensino vs Atitudes Positivas na escala CsA-s

Em relação à cibersegurança fornecida pela escola, os alunos demonstraram uma percepção positiva (como ilustra a figura 23). Em relação à consciencialização, quando são contatados por estranhos, os alunos (figura 24) demonstraram ter um

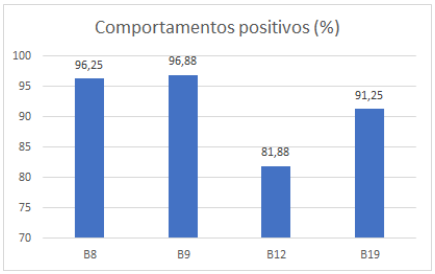


(a) Comportamentos de consciencialização sobre privacidade.

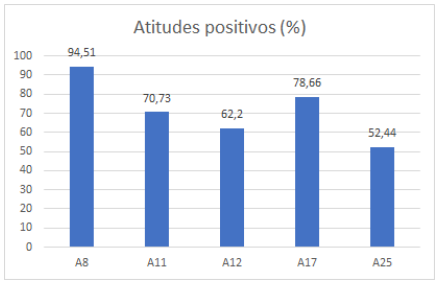


(b) Atitudes de consciencialização sobre privacidade.

Figura 21: Resultado 1 - consciencialização sobre privacidade online



(a) Comportamentos de acesso a serviços de Internet.



(b) Atitudes de acesso a serviços de Internet.

Figura 22: Resultado 2 - Acesso a serviços de Internet

comportamento positivo, como demonstrado no item B17 ao clicarem apenas em links provenientes de pessoas de confiança.

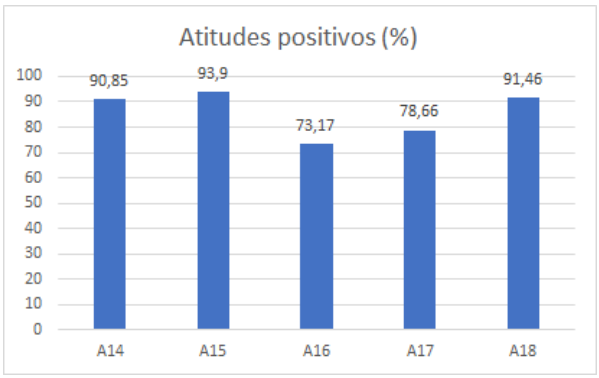


Figura 23: Resultado 3 - Percepção da cibersegurança fornecida pela escola

No resultado 5, analisa-se se os alunos mostraram estar conscientes das suas atitudes (Figura 25a) e comportamentos (Figura 25b) em relação à cibersegurança na escola, o item A7 (*"Os sistemas de computador fornecem toda a proteção de que*

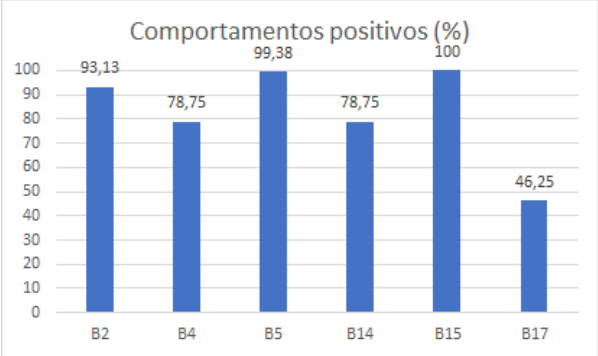
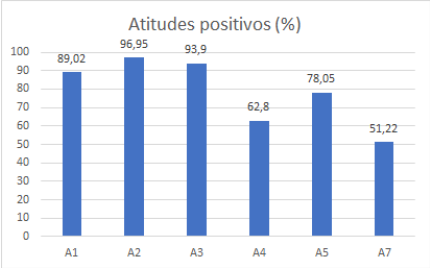
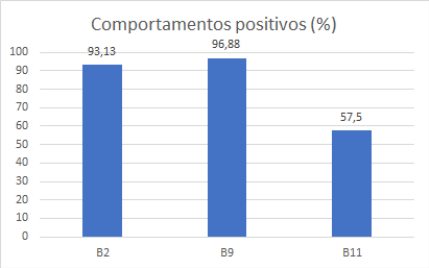


Figura 24: Resultado 4 - Consciencialização quando são contatados por estranhos



(a) Atitudes em relação à cibercegurança na escola.



(b) Comportamentos em relação à cibercegurança na escola.

Figura 25: Resultado 5 - Cibersegurança fornecida pela escola e consciencialização quando são contatados por estranhos

uma escola precisa") e B11 (*"Verificando o software de atualização"*) apresentam os menores valores positivos, 51% e 58%, respetivamente.

No resultado 6, são analisadas as atitudes relacionadas com a compreensão da motivação do cibercriminoso (figura 26), tendo-se concluído que, globalmente, são positivas, e onde o item A22 ("Os cibercriminosos só visam uma escola quando há um ganho financeiro substancial") apresentou o menor valor para atitude positiva (52%). Outro dos aspetos analisados foram as atitudes relacionadas com a aplicação da lei e desempenho dos técnicos de TIC (figura 27), concluindo-se que são positivas, tendo o item A10 ("Os cibercriminosos são mais avançados do que as pessoas que deveriam estar nos protegendo") apresentado o valor positivo mais baixo com apenas (31%).

No resultado 8, foi analisado se os alunos estão atentos à proteção de seus equipamentos e dados (figura 28), concluindo-se que sim, porém no item B18, relacionado com a verificação de atualizações para antivírus, apresentam um comportamento positivo muito baixo com apenas 38%.

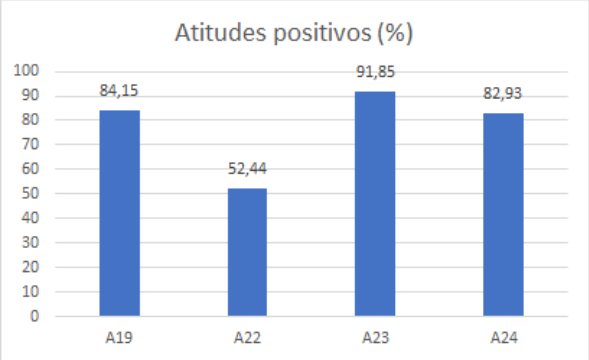


Figura 26: Resultado 6 - Atitudes de compreensão das motivações dos cibercriminosos

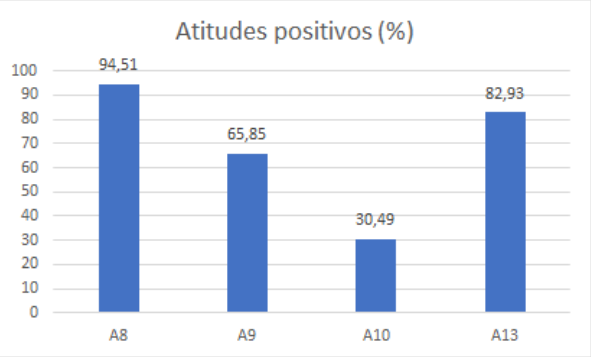


Figura 27: Resultado 7 - Atitudes relacionadas com a aplicação da lei e técnicos de TIC

No resultado 9 (figura 29), alunos mostraram ter um comportamento positivo sobre o uso de software não oficial e protegido contra cópia e gravação.

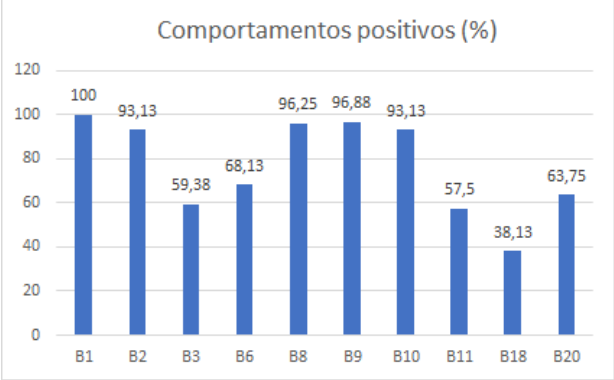


Figura 28: Resultado 8 - Os alunos estão cientes sobre como proteger os seus equipamentos e dados

A distribuição da pontuação global de comportamentos está representada na figura 30, onde se observou uma distribuição enviesada positiva onde 75% dos alunos obtiveram pontuação global até 50 (figura 31), num intervalo de valores que pode variar entre 20-140 e onde valores baixos representam comportamentos positivos.

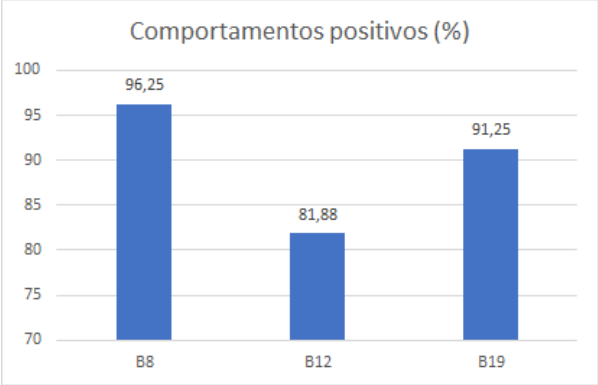


Figura 29: Resultado 9 - Utilização de software não oficial e protegido contra cópia-gravação

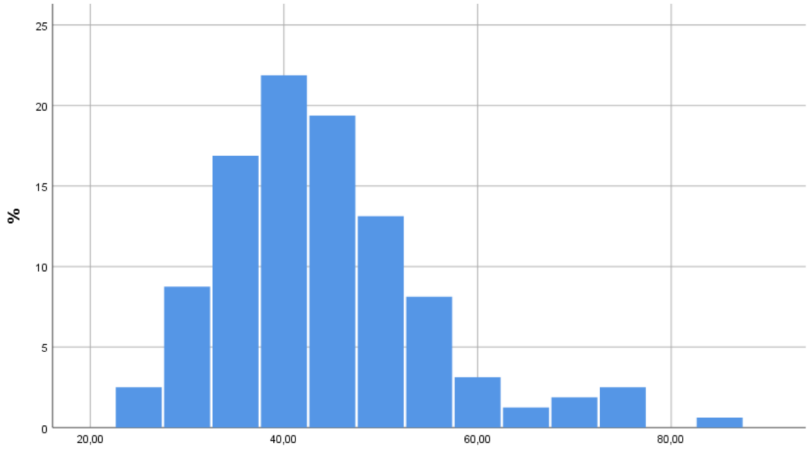


Figura 30: Distribuição da pontuação global no questionário de comportamentos.

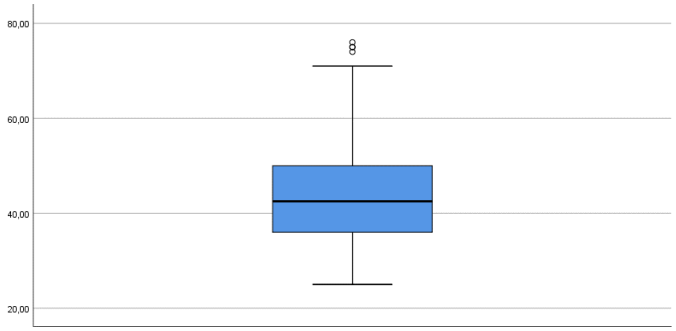


Figura 31: Pontuação global no questionário de comportamentos.

A figura 32 ilustra a distribuição da pontuação global de atitudes onde valores altos representam boas atitudes, tendo-se obtido um valor global de 76 (figura 33) de uma variação possível entre 25 e 100 o que mostra uma atitude global positiva dos alunos.

A figura 34 mostra a distribuição das pontuações globais atingidas para os comportamentos. Observando o valor médio de pontuação global entre os sexos

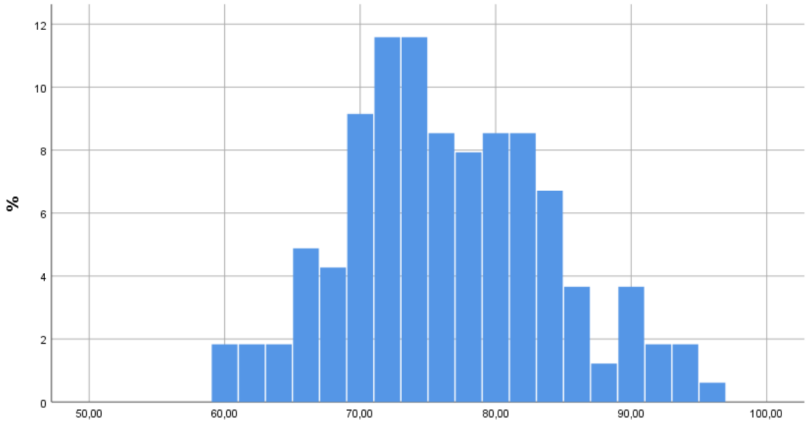


Figura 32: Distribuição da pontuação global no questionário de atitudes.

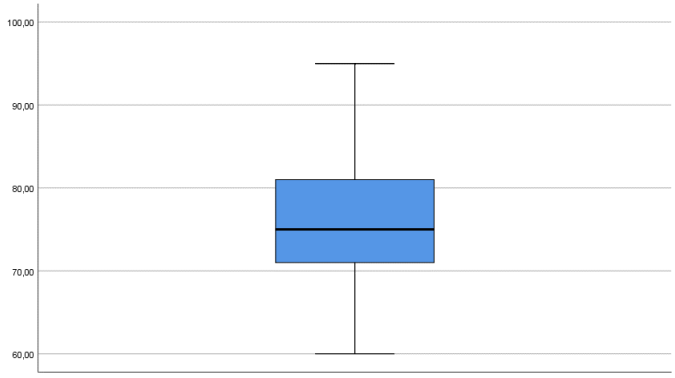


Figura 33: Pontuação global no questionário de atitudes.

foram encontradas diferenças significativas com o género feminino a apresentar comportamentos de menor risco.

A figura 35 apresenta a distribuição das pontuações globais obtidas nas atitudes. São visíveis diferenças significativas com os alunos do 6.º ano a apresentarem atitudes positivas mais expressivas.

Com base nos resultados das perguntas anteriores, não se pode concluir que os alunos dominam de forma natural o uso das novas tecnologias. É possível concluir que numa sociedade com uma dimensão tecnológica crescente e abrangente, embora os alunos apresentem algum domínio na componente de manuseamento técnico, estes necessitam de desenvolver competências humanas como comportamentos, atitudes, pensamento crítico e outros para se manterem seguros online.

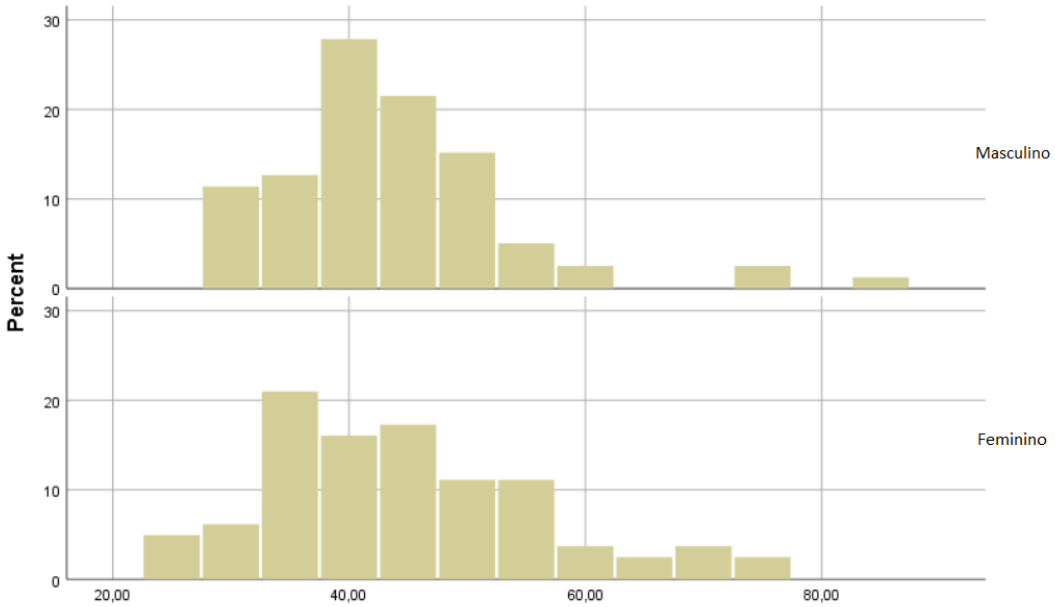


Figura 34: Distribuição da pontuação global de comportamentos por género.

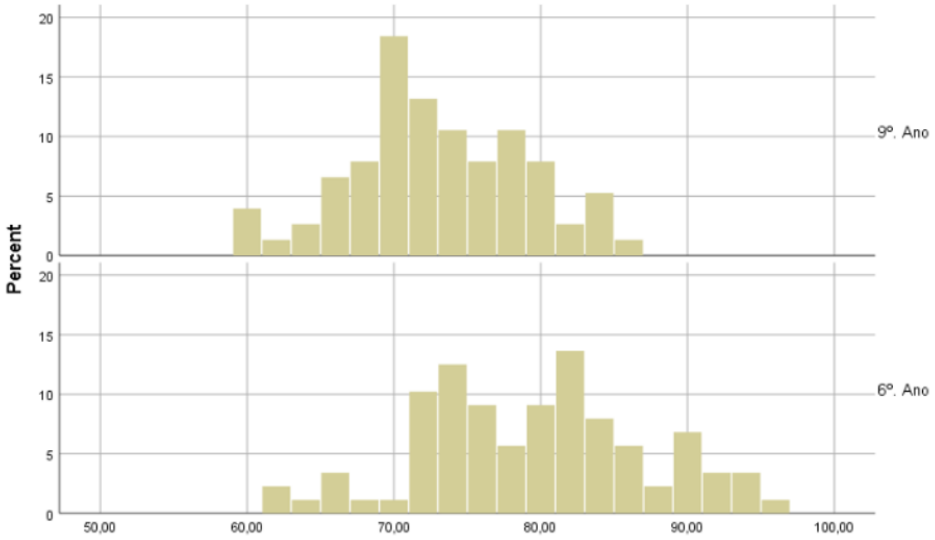


Figura 35: Distribuição da pontuação global de atitudes por ano.

5

CONCLUSÕES

Este trabalho descreve uma estratégia integrada de cibersegurança e consciencialização em contexto escolar. É composto por avaliações de atitudes e comportamentos de risco, um questionário de autodiagnóstico e um plano de aula. O trabalho foi implementado e testado no Colégio Conciliar de Maria Imaculada, com os alunos finalistas do 2.º e 3.º ciclos (6.º e 9.º anos). A avaliação de atitudes e comportamentos de risco de cibersegurança foi realizada com a aplicação dos questionários CsA-S e CsB-S, tendo recolhido 164 respostas. Os mesmos alunos também testaram o questionário de autodiagnóstico e beneficiaram da implementação de um plano de aula direcionado para a cidadania digital. Considerando que qualquer programa de ciberconsciencialização aplicado em contexto escolar deve ser transversal, deverá incluir, a administração, os alunos, o corpo técnico e o corpo docente para que o estudo seja mais completo.

Começou-se por elucidar a administração escolar sobre a necessidade de integrar tópicos de cibersegurança nos currículos e avaliar os comportamentos e atitudes de risco dos alunos.

Os três principais argumentos apresentados foram:

- A escola é uma instituição secular que tem como principal função educar e ensinar crianças e jovens, ajudando-os a adquirir uma grande diversidade de competências. Considerando a crescente utilização de tecnologia e a digitalização dos serviços, é particularmente importante que os alunos tenham competências digitais que lhes permitam uma utilização segura da tecnologia. A escola deve contribuir para a construção da consciência cibernética e aquisição de competências digitais auxiliando os alunos na aquisição da consciência sobre os riscos do uso de dispositivos ligados à Internet mas também consciencializando-os para os comportamentos e atitudes de risco e medidas de ciberconsciência a adotar.
- A avaliação de cibersegurança é necessária em contexto académico, permitindo avaliar e melhorar o nível de cibersegurança da instituição, disponibilizando informação que permite o desenvolvimento de programas de aprendizagem direcionados a professores, funcionários e alunos.

- A ciberconsciencialização nas escolas deve ser vista como um esforço coletivo, envolvendo toda a comunidade escolar (alunos, pais, funcionários, professores e administração). Uma indicação positiva dada pela administração a toda a comunidade representa um passo importante para o sucesso da aplicação de programas de consciencialização em cibersegurança em contexto escolar.

O nível de consciência de cibersegurança da administração escolar, dos alunos e dos pais foi desafiante, dado o baixo nível de consciência da importância da problemática e do impacto positivo de uma avaliação para aprimorar as habilidades de cibersegurança dos alunos. Com a realização desta pesquisa e a publicação dos resultados, procurou-se sensibilizar a comunidade educativa sobre a necessidade de implantação de estratégias de cibersegurança quer na escola quer junto das famílias.

5.1 TRABALHO FUTURO

Com base no trabalho desenvolvido, surgiram novas ideias e sugestões para trabalhos futuros que podem vir a ser um complemento ao trabalho atual.

Desta forma, como trabalho futuro, propõe-se a promoção e divulgação dos questionários de avaliação de atitudes e comportamentos em outras escolas da comunidade. Esta iniciativa permitirá melhorar o que pode ser medido, enriquecendo os dados e constituirá um instrumento adicional de gestão para as autoridades educativas de promoção da segurança cibernética e os hábitos de ciberhigiene nas escolas.

Propõe-se também que este trabalho de sensibilização seja divulgado junto dos níveis de ensino envolvidos na aplicação do questionário, assim como nas escolas secundárias e junto dos pais, professores, funcionários e administração das instituições.

Em relação ao questionário de autodiagnóstico, o conjunto de perguntas pode ser melhorado e ajustado para ir ao encontro de novas realidades e enriquecer o portefólio de perguntas. A informação recolhida no questionário de autodiagnóstico deve ser analisada com o intuito de avaliar os conhecimentos de ciberconsciencialização dos inquiridos, identificando lacunas que necessitem de ser trabalhadas.

A gamificação do questionário de autodiagnostico, aplicada a uma situação que é vista como não divertida, poderá ser uma boa alternativa para aproveitar os desejos naturais de aprendizagem, domínio, competição, realização, reconhecimento e recompensas dos jogadores. Com o desenvolvimento de uma versão para dispositivos

móveis com mecanismo de recompensa, de completar tarefas de cibersegurança num tempo definido, poderá disseminar o uso contínuo e amplo da aplicação móvel de avaliação da cibersegurança.

O plano de aula foi aplicado mas tornou-se evidente a necessidade de uma implementação e aplicação mais ampla, existindo por isso a necessidade de uma nova planificação onde a duração adotada deve ser estendida. Propõe-se, assim, a planificação de um conjunto de aulas sobre cibersegurança a serem incluídas no currículo a lecionar aos alunos na disciplina de Tecnologias de Informação e Comunicação (TIC) ou Cidadania e Desenvolvimento. Da mesma forma, devem ser planeadas sessões autónomas de sensibilização destinadas ao pessoal e professores da instituição, a serem ministradas durante o ano letivo, com o intuito de melhorar as suas habilidades de ciberconsciencialização, reduzindo os riscos de segurança cibernética.

5.2 LIMITAÇÕES

Estando este estudo integrado num projeto académico, a sua implementação teve limitações temporais que foram agravadas pela pandemia de COVID-19.

Com efeito, foi necessário um adiamento da disponibilização e recolha de respostas aos questionários, por se entender ser imprescindível a sua realização em regime presencial. Foi assim possível fazer a apresentação do tema e dos objetivos, bem como o esclarecimento de qualquer dúvida que surgiram aquando da aplicação dos inquéritos.

Por outro lado, foram utilizados dois questionários distintos, um para as atitudes (CsA-S) e outro para os comportamentos (CsB-S) e, sendo estes de caráter anónimo, não foi possível relacioná-los.

Tendo em conta o contexto de aplicação numa escola piloto, a dimensão da amostra é relativamente reduzida, o que poderá ter limitado o âmbito da medição, com as respostas recolhidas.

Dado o tempo limitado de duração deste projeto e a data de disponibilização do questionário de autodiagnostico, não foi possível verificar o tipo de adesão e eficácia do mesmo, como teria sido desejável.

5.3 CONSIDERAÇÕES PESSOAIS

É com grande satisfação e orgulho que dou por terminado o meu projeto, cujos objetivos definidos na introdução foram concretizados com sucesso. Foi uma caminhada longa, mas desafiante. O tema é algo que me move diariamente e que faz parte do meu dia-a-dia profissional. Procurei estar atento às muitas solicitações a que os nossos adolescentes estão sujeitos, não só no meio escolar, como no meio familiar e espero ter contribuído para melhorar a proteção no mundo digital.

De modo a avaliar os comportamentos e as atitudes dos alunos face à cibersegurança, e assim poder ajudá-los a uma autoconsciencialização, disponibilizei, para o efeito, dois questionários de medição dos comportamentos e das atitudes em contexto escolar.

Com a análise dos dados recolhidos e dos elementos de caraterização da população, julgo ter conseguido identificar padrões úteis à criação de conteúdos e estratégias de educação e sensibilização em matéria de cibersegurança.

Pretendi também que os utilizadores fizessem uma autoavaliação dos seus conhecimentos (com o questionário de autodiagnostico), facultado no final uma pontuação e uma lista de recomendações, tendo em conta as respostas obtidas para possíveis leituras futuras.

Apostei ainda no desenvolvimento de um plano de aula de 90 minutos, passível de ser aplicado em disciplinas onde a ciberconsciencialização seja abordada de forma transversal. Esta iniciativa, que considero ser de uma extrema importância, visa desenvolver competências de Cidadania digital, daí a necessidade de implementar o plano nas disciplinas de Educação para a Cidadania e/ou TIC, permitindo envolver a comunidade educativa e não apenas os docentes das disciplinas tecnológicas. É fundamental passar a incluir, a curto-médio prazo, as questões relacionadas com a cibersegurança nos planos de trabalhos de disciplinas com menor cariz tecnológico.

Todos nós somos agentes educativos!

BIBLIOGRAFIA

6dg.co.uk (jan. de 2021). URL: https://www.6dg.co.uk/blog/cybercrime-trends/.

Antunes, Mário et al. (2021). «Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal». Em: *Journal of Cybersecurity and Privacy* 1.2, pp. 219–238.

Barbas, João Manuel Assis e Carolina Sancho Hirane (2018). *Cibersegurança e políticas públicas análise comparada dos casos chileno e português*.

Boletsis, Costas et al. (2021). «Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment». Em: *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2021), Vienna, Austria*, pp. 8–10.

Caldas, Alexandre e Vicente Freire (2013). *Cibersegurança: das preocupações à ação*. JSTOR.

Canongia, Claudia e Raphael Mandarino Junior (2010). «Segurança cibernética: o desafio da nova Sociedade da Informação». Em: *Parcerias Estratégicas* 14.29, pp. 21–46.

Capelão, Filipa e Hugo Barbosa (2018). «Cybersecurity in Healthcare: Risk Analysis in Health Institution in Portugal». Em: *International Journal for Research & Development in Technology (IJRDT)* 9, p. 3.

Capobianco, Ligia (2010). «A revolução em curso: Internet, Sociedade da Informação e Cibercultura». Em: *Estudos em comunicação* 2.7, pp. 175–193.

Carvalho, João Vidal, Sandro Carvalho e Álvaro Rocha (2020). «European strategy and legislation for cybersecurity: implications for Portugal». Em: *Cluster Computing*, pp. 1–10.

Chen, Irene Linlin e Libi Shen (2019). «Cybercitizens at schools». Em: *Emerging trends in cyber ethics and education*. IGI Global, pp. 91–117.

Cibersegurança Portugal, Centro Nacional de (2019). *Quadro Nacional de Referência para a Cibersegurança*. URL: https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf.

— (dez. de 2020). *Relatório Cibersegurança em Portugal – Sociedade 2020*. Rel. téc. Centro Nacional de Cibersegurança Portugal.

Cibersegurança Portugal, Centro Nacional de (mai. de 2021). URL: https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2021__observatoriociberseguranca_cncs.pdf.

Conselho de Ministros, Presidência do (2019).

Conselho de Ministros n.º 137/2007, Resolução do (set. de 2007). *Plano Tecnológico da Educação*. URL: https://dre.pt/pesquisa/-/search/642198/details/maximized.

CSIRT – Grupo de Trabalho Taxonomia, Rede Nacional de (jan. de 2020). *Taxonomia Comum da Rede Nacional de CSIRT*. V3.0 ENISA / TF-CSIRT RSTI WG v.1002. URL: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf.

ENISA (nov. de 2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. URL: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

— (out. de 2020). *ENISA Threat Landscape 2020 - Main Incidents*. Rel. téc. ENISA.Europa.eu. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport.

Europol (nov. de 2020). *COVID-19 sparks upward trend in cybercrime*. URL: https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime.

Fernandes, José Pedro Teixeira (2012). «Utopia, liberdade e soberania no ciberespaço». Em: *Nação e defesa* 133, pp. 11–31.

Furnell, Steven et al. (2018). «Enhancing security behaviour by supporting the user». Em: *Computers & Security* 75, pp. 1–9.

Gonçalves, Rita Santos (2019). «O fator humano da cibersegurança nas organizações». Tese de doutoramento. Instituto Superior de Economia e Gestão.

Hadlington, Lee (2017). «Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours». Em: *Heliyon* 3.7, e00346.

Hanus, Bartlomiej e Yu "Andy" Wu (2016). «Impact of users security awareness on desktop security behavior: A protection motivation theory perspective». Em: *Information Systems Management* 33.1, pp. 2–16.

I.Arends, Richard (jun. de 2008). *Aprender a ensinar*. seventh. ISBN:978-84-481-6010-4. Mcgraw-Hill Higher Education.

KEMP, SIMON (2021). *DIGITAL 2021 GLOBAL OVERVIEW REPORT*. Rel. téc. https://hootsuite.widen.net/s/zcdrtxwczn/digital2021$_g$*lobalreport*$_e$*n*: Hootsuite.

Kemp, Simon (2020). «Digital 2020: 3.8 billion people use social media». Em: *We Are Social and Hootsuite, Digital Report*.

Kilic, Figen e Ismail Karakuş (2021). «New Features of Learners in Education: Digital Awareness, Digital Competence, and Digital Fluency». Em: *Improving Scientific Communication for Lifelong Learners*. IGI Global, pp. 113–132.

Kohn, Karen e CH de Moraes (2007). «O impacto das novas tecnologias na sociedade: conceitos e caracterısticas da Sociedade da Informação e da Sociedade Digital». Em: *XXX Congresso Brasileiro de Ciências da Comunicação*. Vol. 30. 3, pp. 1–13.

Kritzinger, Elmarie e Sebastiaan H von Solms (2010). «Cyber security for home users: A new way of protection through awareness enforcement». Em: *Computers & Security* 29.8, pp. 840–847.

Leidner, Dorothy E (2020). «Editorial reflections: Lockdowns, slow downs, and some introductions». Em: *Journal of the Association for Information Systems* 21.2, p. 10.

Livingstone, Sonia et al. (2011). «Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries». Em:

McCormac, Agata et al. (2017). «Individual differences and information security awareness». Em: *Computers in Human Behavior* 69, pp. 151–156.

Mee, Paul, Rico Brandenburg e Wenhan Lin (set. de 2020). «Oliver Wyman Forum Global Cyber Risk Literacy and Education Index». Em:

Microsoft (2020a). *Empowering and securing your Firstline Workforce eBook*. URL: https://azure.microsoft.com/pt-pt/resources/empowering-and-securing-your-firstline-workforce-ebook/.

— (set. de 2020b). *Microsoft Digital Defense Report*. Rel. téc. URL: https://www.microsoft.com/en-us/security/business/security-intelligence-report.

Mittal, Sandeep (2015). «Understanding the human dimension of cyber security». Em: *Indian Journal of Criminology & Criminalistics (ISSN 0970–4345)* 34.1, pp. 141–152.

Mouton, Francois et al. (2014). «Social engineering attack framework». Em: *2014 Information Security for South Africa*. IEEE, pp. 1–9.

Peker, Yesem, Lydia Ray e Stephanie da Silva (2018). «Online Cybersecurity Awareness Modules for College and High School Students». Em: *2018 National Cyber Summit (NCS)*. IEEE, pp. 24–33.

Pfleeger, Shari Lawrence e Deanna D Caputo (2012). «Leveraging behavioral science to mitigate cyber security risk». Em: *Computers & security* 31.4, pp. 597–611.

Portugal, INE (2020). *Aumentaram significativamente os utilizadores de internet e de comércio eletrónico. Mais que duplicou a percentagem dos utilizadores por motivos educativos - 2020*. URL: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415622225&DESTAQUESmodo=2&xlang=pt.

proofpoint.com (2019). *The Human Factor 2019*. Rel. téc. 0819-032. proofpoint. URL: https://www.proofpoint.com/us/resources/threat-reports/human-factor.

Rahman, A et al. (2020). «The importance of cybersecurity education in school». Em: *Int. J. Inf. Educ. Technol* 10.5, pp. 378–382.

República, Gabinete Cibercrime Procuradoria-Geral da (2020). *COVID 19: CIBERCRIME EM TEMPO DE PANDEMIA*. Rel. téc. Ministério Público Portugal. URL: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/cibercrime_em_tempo_de_pandemia-20-04-2020.pdf.

Richardson, Michael D et al. (2020). «Planning for Cyber Security in Schools: The Human Factor.» Em: *Educational Planning* 27.2, pp. 23–39.

Sabillon, Regner, Jordi Serra-Ruiz, Victor Cavaller et al. (2019). «An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada». Em: *Journal of Cases on Information Technology (JCIT)* 21.3, pp. 26–39.

Al-Sartawi, Abdalmuttaleb MA Musleh (2020). «Information technology governance and cybersecurity at the board level». Em: *International Journal of Critical Infrastructures* 16.2, pp. 150–161.

Sen, Ravi (2018). «Challenges to cybersecurity: Current state of affairs». Em: *Communications of the Association for Information Systems* 43.1, p. 2.

Silva, Maria Helena Santos e José Pinto Lopes (2016). «Três estratégias básicas para a melhoria da aprendizagem: Objetivos de aprendizagem, avaliação formativa e feedback». Em: *Revista eletrónica de Educação e Psicologia* 7, pp. 12–31.

Silva Lopes Nunes, Paulo Manuel Roque da (2019). «Avaliação das atitudes e comportamentos de cibersegurança dos profissionais de saúde em ambiente hospitalar». Tese de doutoramento. Instituto Politécnico de Lisboa, Escola Superior de Tecnologia da Saúde de ...

Singh, Prabhsimran et al. (2020). «Psychological fear and anxiety caused by COVID-19: Insights from Twitter analytics». Em: *Asian Journal of Psychiatry* 54, p. 102280.

Slusky, Ludwig e Parviz Partow-Navid (2012). «Students information security practices and awareness». Em: *Journal of Information Privacy and Security* 8.4, pp. 3–26.

Smahel, David et al. (2020). «EU Kids Online 2020: Survey results from 19 countries». Em:

Tirumala, Sreenivas Sremath, Abdolhossein Sarrafzadeh e Paul Pang (2016). «A survey on Internet usage and cybersecurity awareness in students». Em: *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, pp. 223–228.

Zook, Chris (dez. de 2019).

Zwilling, Moti, Galit Klien et al. (2020). «Cyber security awareness, knowledge and behavior: a comparative study». Em: *Journal of Computer Information Systems*, pp. 1–16.

Zwilling, Moti, Dušan Lesjak et al. (2019). «How to deal with the awareness of cyber hazards and security in (Higher) education». Em: *Thriving on future education, industry, business and society. Proceedings of the Makelearn and TIIM International Conference*, pp. 433–439.

APÊNDICES

A

APÊNDICE A - DOCUMENTOS RELACIONADOS COM OS QUESTIONÁRIOS

A.1 PEDIDO DE REALIZAÇÃO DO ESTUDO NA ESCOLA

Solicitação de autorização para realização de Inquérito

Frederico Manuel Ferreira Marques <2190377@my.ipleiria.pt>

sex, 09/10/2020 21:33

Para: direcao@ccmi.com.pt <direcao@ccmi.com.pt>
Cc: Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>

Exmo Senhor Diretor Pedagógico do Colégio Conciliar de Maria Imaculada, Doutor Jorge Cotovio

O meu nome é Frederico Manuel Ferreira Marques, e sou estudante do 2ºano do Mestrado em Cibersegurança e Informática Forense (MCIF) da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.
Encontro-me atualmente a desenvolver os trabalhos da dissertação sob a orientação do Professor Doutor Mário Antunes, onde se pretende avaliar os comportamentos e atitudes dos estudantes, professores e funcionários relativamente à cibersegurança.
O trabalho será realizado junto da comunidade escolar do ensino básico e secundário. Nesse sentido, pretende-se realizar um inquérito com fundamentação científica, que recolha informação sobre os comportamentos e atitudes dos utilizadores quando utilizam a Internet.
O público alvo identificado para este inquérito são os alunos do 9ºano e os funcionários docentes e não-docentes.
O questionário será previamente validado e seguirá os requisitos do Regulamento Geral de Proteção de Dados.

Tendo em conta a sensibilidade do CCMI para as questões da segurança informática, venho pelo presente solicitar autorização para a realização do respetivo questionário aos alunos do 9ºano e aos funcionários docentes e não docentes do CCMI. As respostas são anónimas e não haverá identificação pessoal das pessoas que participarem.
Havendo autorização, o CCMI será a instituição piloto para este estudo, onde se obterá uma visão global do nível de cibersegurança da comunidade e a identificação de medidas a adotar para mitigar esse risco, nomeadamente ao nível de estratégias de ciber-higiene e consciencialização para as questões relacionadas com cibersegurança.
Os resultados globais do estudo serão disponibilizados na dissertação de mestrado.

Agradeço desde já a atenção dada a este assunto e encontro-me disponível para eventuais esclarecimentos que considerem necessários.

Com os Melhores Cumprimentos

Frederico Marques

A.2 AUTORIZAÇÃO PARA REALIZAR O ESTUDO NA ESCOLA

Re: Solicitação de autorização para realização de Inquérito

Direção CCMI <direcao@ccmi.com.pt>
sex, 09/10/2020 22:22

Para: Frederico Manuel Ferreira Marques <2190377@my.ipleiria.pt>
Cc: Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>

Caro Frederico, estando salvaguardadas todas as questões relativas à privacidade, estaremos, naturalmente, disponíveis para colaborar.
Antes de darmos início ao processo, gostaria de ver o questionário.
Um abraço,
Jorge Cotovio

Frederico Manuel Ferreira Marques <2190377@my.ipleiria.pt> escreveu no dia sexta, 9/10/2020 à(s) 21:33:

> Exmo Senhor Diretor Pedagógico do Colégio Conciliar de Maria Imaculada, Doutor Jorge Cotovio
>
> O meu nome é Frederico Manuel Ferreira Marques, e sou estudante do 2ºano do Mestrado em Cibersegurança e Informática Forense (MCIF) da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.
> Encontro-me atualmente a desenvolver os trabalhos da dissertação sob a orientação do Professor Doutor Mário Antunes, onde se pretende avaliar os comportamentos e atitudes dos estudantes, professores e funcionários relativamente à cibersegurança.
> O trabalho será realizado junto da comunidade escolar do ensino básico e secundário. Nesse sentido, pretende-se realizar um inquérito com fundamentação científica, que recolha informação sobre os comportamentos e atitudes dos utilizadores quando utilizam a Internet.
> O público alvo identificado para este inquérito são os alunos do 9ºano e os funcionários docentes e não-docentes.
> O questionário será previamente validado e seguirá os requisitos do Regulamento Geral de Proteção de Dados.
>
> Tendo em conta a sensibilidade do CCMI para as questões da segurança informática, venho pelo presente solicitar autorização para a realização do respetivo questionário aos alunos do 9ºano e aos funcionários docentes e não docentes do CCMI. As respostas são anónimas e não haverá identificação pessoal das pessoas que participarem.
> Havendo autorização, o CCMI será a instituição piloto para este estudo, onde se obterá uma visão global do nível de cibersegurança da comunidade e a identificação de medidas a adotar para mitigar esse risco, nomeadamente ao nível de estratégias de ciber-higiene e consciencialização para as questões relacionadas com cibersegurança.
> Os resultados globais do estudo serão disponibilizados na dissertação de mestrado.
>
> Agradeço desde já a atenção dada a este assunto e encontro-me disponível para eventuais esclarecimentos que considerem necessários.
>
> Com os Melhores Cumprimentos
>
> Frederico Marques

A.3 PEDIDO DE AUTORIZAÇÃO PARA UTILIZAÇÃO DAS ESCALAS

Request to apply and translate your scales ATC-IB and RScB

Frederico Manuel Ferreira Marques <2190377@my.ipleiria.pt>

qua, 04/11/2020 22:48

Para: lee.hadlington@ntu.ac.uk <lee.hadlington@ntu.ac.uk>; lhadlington@dmu.ac.uk <lhadlington@dmu.ac.uk>
Cc: Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>

Dear Prof. Lee Hadlington,

My name is Frederico Marques, and I am currently a 2nd year student of the MSc in Cybersecurity and Computer Forensics at the School of Technology and Management of the Polytechnic of Leiria (https://www.ipleiria.pt/cursos/course/master-in-cybersecurity-and-digital-forensics/).

I am currently developing my dissertation work under the supervision of Professor Mário Antunes.
The dissertation aims to assess and evaluate the behaviors and attitudes of 9th grade students and teachers towards cybersecurity, in a portuguese school.
In this sense, I would like to ask you for authorization to apply and translate for portuguese your scales ATC-IB and RScB, published in: Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346.

The questionnaires will only be used under the scope of my thesis work and any publication and dissemination of the results will cite the original paper indicated above.

I thank you in advance and I'll look forward to your answer.

Kind Regards,

Frederico Marques

A.4 AUTORIZAÇÃO DE UTILIZAÇÃO DAS ESCALAS

Re: Request to apply and translate your scales ATC-IB and RScB

Hadlington, Lee <lee.hadlington@ntu.ac.uk>
seg, 09/11/2020 09:36

Para: Frederico Manuel Ferreira Marques <2190377@my.ipleiria.pt>; lhadlington@dmu.ac.uk <lhadlington@dmu.ac.uk>
Cc: Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>

Hello Frederico

I trust this email finds you safe and well ! I am very pleased to hear that you want to use the scales, and I have no problem with you doing so BUT I would mention one thing, the ATC-IB is more intended for a group of individuals working within in an organisation, and asks specific questions that might need to be 'tweaked' for student population – for example, the questions about 'management' etc perhaps won't make much sense to a student cohort ?

It might be worth thinking about this from the ground up and perhaps trying to develop a hybrid scale that taps into student attitudes towards cybersecurity and information security awareness – I extend an offer of additional help if needed

Best

Lee

Dr Lee Hadlington BSc (Hons) PhD FHEA CPsychol
Senior Lecturer In Cyberpsychology

Chaucer Building Room 432
Nottingham Trent University,
50 Shakespeare Street,
Nottingham. NG1 4FQ
Telephone: +44 (0)115 XXX XXXX
Email: lee.hadlington@ntu.ac.uk

NTU Nottingham Trent University
School of Social Sciences

From: Frederico Manuel Ferreira Marques <2190377@my.ipleiria.pt>
Date: Wednesday, 4 November 2020 at 22:48
To: Hadlington, Lee <lee.hadlington@ntu.ac.uk>, lhadlington@dmu.ac.uk <lhadlington@dmu.ac.uk>

Cc: Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>
Subject: Request to apply and translate your scales ATC-IB and RScB

Dear Prof. Lee Hadlington,

My name is Frederico Marques, and I am currently a 2nd year student of the MSc in Cybersecurity and Computer Forensics at the School of Technology and Management of the Polytechnic of Leiria (https://www.ipleiria.pt/cursos/course/master-in-cybersecurity-and-digital-forensics/).

I am currently developing my dissertation work under the supervision of Professor Mário Antunes.
The dissertation aims to assess and evaluate the behaviors and attitudes of 9th grade students and teachers towards cybersecurity, in a portuguese school.
In this sense, I would like to ask you for authorization to apply and translate for portuguese your scales ATC-IB and RScB, published in: Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346.

The questionnaires will only be used under the scope of my thesis work and any publication and dissemination of the results will cite the original paper indicated above.

I thank you in advance and I'll look forward to your answer.

Kind Regards,

Frederico Marques

A.5 PEDIDO DE COLABORAÇÃO A ESPECIALISTAS

pedido de comentários

Frederico Manuel Ferreira Marques <2190377@my.ipleiria.pt>

seg, 21/12/2020 14:00

Para: Baltazar Manuel Proença Rodrigues <baltazar.rodrigues@ipleiria.pt>
Cc: Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>

Caro Professor Baltazar Rodrigues,

Espero que esta mensagem o encontre bem.

O meu nome é Frederico Marques, estou atualmente a desenvolver os trabalhos conducentes à dissertação do Mestrado em Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria, sob orientação do Professor Mário Antunes.

O trabalho em curso pretende avaliar o risco dos comportamentos e atitudes dos alunos do ensino básico (6º e 9º anos de escolaridade) face à cibersegurança.

Nesse sentido, tenho trabalhado na tradução e adaptação de duas escalas já publicadas e avaliadas, nomeadamente a ATC-IB e RScB:

Hadlington, Lee. "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours." Heliyon 3.7 (2017): e00346. O artigo encontra-se disponível em https://www.sciencedirect.com/science/article /pii/S2405844017309982.

Uma vez que a versão inicial das escalas ATC-IB e RScB foi orientada para o meio empresarial, algumas das perguntas necessitaram de um ajustamento ao contexto escolar onde se desenvolve o presente trabalho.

Como resultado obteve-se uma nova versão das escalas, que carece de validação e aprovação por um grupo de peritos.

Nesse sentido, gostaria de solicitar a sua colaboração como perito em cibersegurança, partilhando as suas sugestões e propostas de alteração na redação das perguntas das escalas adaptadas, bem como um comentário global.

O acesso às referidas escalas é feito online, através dos seguintes links e respetivos códigos de acesso:

1) Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB) com adaptações para escolas:
https://cyberawarenessk12.limequery.com/438481?lang=pt
código de acesso: mvNrO3o2GI7UHeC

2) Risky Cybersecurity Behaviours Scale (RScB) com adaptações para escolas:
https://cyberawarenessk12.limequery.com/414918?lang=pt
código de acesso: FSiHdqhkiq0BlY6

As respostas podem ser guardadas e o inquérito retomado no ponto onde terminou clicando em "Continuar mais tarde" até à submissão final do formulário.

Tendo em conta o plano de trabalhos definido para a dissertação, agradecia o seu contributo até ao próximo dia 24/01/2021.

Agradeço desde já a sua disponibilidade e encontro-me disponível para eventuais esclarecimentos que julgue necessários.

Aproveito ainda para lhe desejar boas festas.

Cumprimentos
Frederico Marques
(2190377@my.ipleiria.pt)

pedido de comentários

Frederico Manuel Ferreira Marques <2190377@my.ipleiria.pt>

seg, 21/12/2020 14:00

Para: Carlos Manuel da Silva Rabadão <carlos.rabadao@ipleiria.pt>
Cc: Mário João Gonçalves Antunes <mario.antunes@ipleiria.pt>

Caro Professor Carlos Rabadão,

Espero que esta mensagem o encontre bem.

O meu nome é Frederico Marques, estou atualmente a desenvolver os trabalhos conducentes à dissertação do Mestrado em Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria, sob orientação do Professor Mário Antunes.

O trabalho em curso pretende avaliar o risco dos comportamentos e atitudes dos alunos do ensino básico (6º e 9º anos de escolaridade) face à cibersegurança.

Nesse sentido, tenho trabalhado na tradução e adaptação de duas escalas já publicadas e avaliadas, nomeadamente a ATC-IB e RScB:

Hadlington, Lee. "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours." Heliyon 3.7 (2017): e00346. O artigo encontra-se disponível em https://www.sciencedirect.com/science/article/pii/S2405844017309982.

Uma vez que a versão inicial das escalas ATC-IB e RScB foi orientada para o meio empresarial, algumas das perguntas necessitaram de um ajustamento ao contexto escolar onde se desenvolve o presente trabalho.

Como resultado obteve-se uma nova versão das escalas, que carece de validação e aprovação por um grupo de peritos.

Nesse sentido, gostaria de solicitar a sua colaboração como perito em cibersegurança, partilhando as suas sugestões e propostas de alteração na redação das perguntas das escalas adaptadas, bem como um comentário global.

O acesso às referidas escalas é feito online, através dos seguintes links e respetivos códigos de acesso:

1) Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB) com adaptações para escolas:
https://cyberawarenessk12.limequery.com/438481?lang=pt
código de acesso: GikLrDTQz1Q10PN

2) Risky Cybersecurity Behaviours Scale (RScB) com adaptações para escolas:
https://cyberawarenessk12.limequery.com/414918?lang=pt
código de acesso: PieEXX0vJNjRRsz

As respostas podem ser guardadas e o inquérito retomado no ponto onde terminou clicando em "Continuar mais tarde" até à submissão final do formulário.

Tendo em conta o plano de trabalhos definido para a dissertação, agradecia o seu contributo até ao próximo dia 24/01/2021.

Agradeço desde já a sua disponibilidade e encontro-me disponível para eventuais esclarecimentos que julgue necessários.

Aproveito ainda para lhe desejar boas festas.

Cumprimentos
Frederico Marques
(2190377@my.ipleiria.pt)

A.6 SUGESTÕES E PROPOSTAS DE ALTERAÇÃO DOS ESPECIALISTAS NAS ESCALAS ADAPTADAS

A.6.1 *Propostas e observações do Dr. Baltazar Rodrigues*

Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB) com adaptações para escolas - comentários dos especialistas

Resposta ao inquérito 1

ID da resposta
2

Data de submissão
1980-01-01 00:00:00

Última página
1

Idioma inicial
pt

Seed
292777635

Código
mvNrO3o2GI7UHeC

Primeiro nome
Baltazar

Último nome
Rodrigues

ATC-IB PT

1 - Ignora avisos de actualizações do software do computador.
Relevante e adequada

2 - Estou ciente do meu papel em manter a escola protegida de potenciais ciberameaças.
Muito abrangente e de entendimento dúbio.

3 - Penso que todos na escola têm um papel a desempenhar na proteção contra as ciberameaças.
Relevante e adequada

4 - É difícil saber como posso proteger a escola do cibercrime.
Relevante e adequada

5 - Não tenho as competências necessárias para proteger a escola do cibercrime.
Idêntica à anterior! É intencional?

6 - Acredito que a informação pessoal não deve ser revelada online, nomeadamente quem sou, onde vivo ou que escola frequento.
Relevante e adequada

7 - Os sistemas de informação oferecem toda a proteção de que uma escola necessita.
Relevante e adequada

8 - Creio que denunciar o cibercrime é uma perda de tempo.
Relevante e adequada

9 - A Autoridade não tem meios para combater o cibercrime de forma eficaz.
Relevante e adequada

10 - Creio que os hackers e cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger.
Relevante e adequada

11 - Faria o download de material abrangido por direitos de autor (imagens, documentos, videos).
Relevante e adequada

12 - Acredito que, quando visualizo conteúdos relacionados com violência em contexto escolar, posso estar a promover a sua partilha e comentários.
Relevante e adequada

13 - Receio que, se denunciar um ciberataque à escola e às autoridades, isso vá prejudicar a reputação da escola.
Relevante mas não deveria ser mais pessoalizada (receio próprio)?

14 - Penso que poderá ser feito mais para comunicar os riscos do cibercrime à comunidade educativa.
Relevante e adequada

15 - Estou a par da política de uso informático da escola e tento segui-la.
Relevante e adequada

16 - Se ocorrer um ciberataque, não saberia como denunciá-lo.
Relevante e adequada

17 - Não acho que é minha responsabilidade denunciar um ciberataque contra a escola.
Relevante e adequada

18 - Não presto atenção ao material informativo da escola sobre ameaças de cibercrime.
Relevante e adequada

19 - Confio na minha capacidade de reconhecer sinais de um ciberataque.
Relevante e adequada

20 - Acredito que quando aparecem conteúdos inapropriados online, devo pedir ajuda a um adulto.
Relevante e adequada

21 - Sinto que qualquer pessoa da escola está em risco de manipulação por ciber "vigaristas e burlões".
Relevante e adequada

22 - Penso que os cibercriminosos e hackers apenas atingem uma escola quando têm muito a ganhar do ponto de vista financeiro.
Relevante e adequada

23 - Apenas as grandes empresas e organizações são alvo dos hackers e cibercriminosos.
Relevante e adequada

24 - Acredito que apenas as instituições que recebem pagamentos por sistemas online estão em risco de serem vítimas de um ciberataque.
Relevante e adequada

25 - Penso que tenho o direito de estar sempre online, com acesso a todos os serviços da Internet.
Relevante e adequada

Comentários finais e observações:
Não faço ideia se no contexto deste projeto é possível, mas penso faria sentido a introdução de algumas sobre quais as entidades a contactar em situação de ciberameaça oiu cibercrime, bem como sobre o conhecimento individual da legislação vigente!

Risky Cybersecurity Behaviours Scale (RScB) com adaptações para escolas - comentários dos especialistas

Survey response 1

Response ID
2

Date submitted
1980-01-01 00:00:00

Last page
1

Start language
pt

Seed
426273508

Token
FSiHdqhkiq0BlY6

First name
Baltazar

Last name
Rodrigues

RScB-PT

1 - Partilhar palavras-passe com colegas.
Relevante e adequada.

2 - Usar ou criar palavras-passe demasiado simples (ex: nome de familiar, data de nascimento, apelidos, sequencias de carateres, menos de 8 digitos).
Relevante e adequada.

3 - Usa a mesma palavra-passe para diferentes websites.
Relevante e adequada.

4 - Usa sistemas de armazenamento online para partilhar ou guardar informação pessoal e sensível(google drive, dropbox, onedrive, etc).
Relevante e adequada.

5 - Inserir informação de pagamento em jogos “Freemium”, que são gratuitos mas que oferecem benefícios mediante pagamento.
Relevante e adequada.

6 - Usar redes Wi-Fi de acesso livre (públicas).
Relevante e adequada.

7 - Confiar num amigo ou colega próximo para conselhos em aspetos de segurança online.
Relevante e adequada.

8 - Descarregar software antivírus gratuito de fontes desconhecidas.
Relevante e adequada.

9 - Desativar o antivírus do computador para que possa descarregar informação de websites.
Relevante e adequada.

10 - Utilizar a pen drive pessoal com a finalidade de transferir informação para os computadores da escola.
Relevante e adequada.

11 - Verificar regularmente as actualizações de software do smartphone/tablet/portátil/PC.
Relevante e adequada.

12 - Descarregar conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas.
Relevante e adequada.

13 - Partilhar a sua localização nas redes sociais. (Fotos, local de férias...).
Relevante e adequada.

14 - Aceitar solicitações de amizade em redes sociais porque reconhece fotos.
Relevante e adequada.

15 - Clicar em links de email não solicitados de uma fonte desconhecida.
Relevante e adequada.

16 - Enviar informação pessoal a estranhos pela Internet (contactos nas redes sociais, darnúmeros de telefone ou email para obter códigos de download ou prémios, etc..).
Relevante e adequada.

17 - Clicar em links de email enviados por amigos próximos ou por colegas de trabalho.
Relevante e adequada.

18 - Verificar atualizações para quaisquer antivírus que tenha instalado.
Relevante e adequada.

19 - Descarregar informação e material de websites para o computador sem verificação da autenticidade.
Relevante e adequada.

20 - Guardar informação pessoal, de familiares e amigos no dispositivo eletrónico pessoal (por ex., smartphone/tablet/portátil).
Relevante e adequada.

Comentários finais e observações:
Excelente - sem comentários

A.6.2 *Propostas e observações do Dr. Carlos Rabadão*

Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB) com adaptações para escolas - comentários dos especialistas

Resposta ao inquérito 1

ID da resposta
1

Data de submissão
1980-01-01 00:00:00

Última página
1

Idioma inicial
pt

Seed
104778311

Código
GikLrDTQz1Q10PN

Primeiro nome
Carlos

Último nome
Rabadão

ATC-IB PT

1 - Ignora avisos de actualizações do software do computador.
Parece-me demasiadamente específica para o início do inquérito. Não tem qualquer ligação com a inicial "I think that management have the responsibility to ensure a company is protected from cybercrime" e que me parece relevante. Deveria ser mantida. No inquérito original parece-me que as atitudes consideradas têm mais a ver com a postura/envolvimento/comprometimento/perceção e que o tipo de atitude desta pergunta está mais relacionado com os riscos provenientes das atitudes dos utilizadores. Por exemplo a utilizaçãoo da mesma pwd em vários sites, que também é uma atitude mas é considerada nos riscos.

2 - Estou ciente do meu papel em manter a escola protegida de potenciais ciberameaças.

3 - Penso que todos na escola têm um papel a desempenhar na proteção contra as ciberameaças.

4 - É difícil saber como posso proteger a escola do cibercrime.
O que se pretende? i) Dizer que não sei como posso ajudar ou ii) Que é difícil obter informação para ajudar Proponho a utilização de "Não sei como contribuir para proteger a escola do cibercrime.

5 - Não tenho as competências necessárias para proteger a escola do cibercrime.

6 - Acredito que a informação pessoal não deve ser revelada online, nomeadamente quem sou, onde vivo ou que escola frequento.
A questão original parece-me bastante relevante e deveria ser mantida. Esta questão também me parece relevante.

7 - Os sistemas de informação oferecem toda a proteção de que uma escola necessita.
Desambiguar "sistemas de informação" -> "sistemas informáticos"

8 - Creio que denunciar o cibercrime é uma perda de tempo.

9 - A Autoridade não tem meios para combater o cibercrime de forma eficaz.
Desambiguar "Autoridade" -> As autoridades de segurança ...

10 - Creio que os hackers e cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger.
O termo hacker têm muitas conotações, "bons", "assim-assim" e "criminosos". Aqui é utilizado como qualquer coisa má. Bastaria cibercriminosos como na questão original.

11 - Faria o download de material abrangido por direitos de autor (imagens, documentos, videos).
A questão original parece-me bastante relevante e deveria ser mantida. Esta questão também me parece relevante.

12 - Acredito que, quando visualizo conteúdos relacionados com violência em contexto escolar, posso estar a promover a sua partilha e comentários.

13 - Receio que, se denunciar um ciberataque à escola e às autoridades, isso vá prejudicar a reputação da escola.
Retirava "à escola", tal como na questão original, pois não impacta na reputação se a escola não tornar o incidente público.

14 - Penso que poderá ser feito mais para comunicar os riscos do cibercrime à comunidade educativa.
Desambiguar "comunicar" -> dar a conhecer/divulgar/sensibilizar

15 - Estou a par da política de uso informático da escola e tento segui-la.
O termo "políticas" é âmbiguo para este público. Para desambiguar proponho "Estou a par das regras de utilização dos recursos informáticos da Escola ..."

16 - Se ocorrer um ciberataque, não saberia como denunciá-lo.
Se ocorrer um ciberataque, não sei/não sabaerei como denunciá-lo.

17 - Não acho que é minha responsabilidade denunciar um ciberataque contra a escola.
Não acho que "seja" ... ciberataque "que tenha sido lançado a partir da Escola".

18 - Não presto atenção ao material informativo da escola sobre ameaças de cibercrime.
Não presto atenção "à informação disponibilizado pela Escola" sobre as ameaças do cibercrime.

19 - Confio na minha capacidade de reconhecer sinais de um ciberataque.
Desambiguar "de reconhecer" -> "para detetar/identificar"

20 - Acredito que quando aparecem conteúdos inapropriados online, devo pedir ajuda a um adulto.

21 - Sinto que qualquer pessoa da escola está em risco de manipulação por ciber "vigaristas e burlões".

22 - Penso que os cibercriminosos e hackers apenas atingem uma escola quando têm muito a ganhar do ponto de vista financeiro.

23 - Apenas as grandes empresas e organizações são alvo dos hackers e cibercriminosos.

24 - Acredito que apenas as instituições que recebem pagamentos por sistemas online estão em risco de serem vítimas de um ciberataque.
Na questão roiginal parece que a intenção é outra "take". Assim, substituir "recebem" -> "utilizam meios de pagamento online"

25 - Penso que tenho o direito de estar sempre online, com acesso a todos os serviços da Internet.
A questão original é importante. Permite saber se os estudantes sabem que é o responsável na Escola pela Cibersegurança.

Comentários finais e observações:
Não sei se não seria de fazer um extensão de 25 para 30 questões. Isto porque as questões retiradas me parecem relevantes para caracterizar os comportamentos organizacionais quanto à cibersegurança.

Risky Cybersecurity Behaviours Scale (RScB) com adaptações para escolas - comentários dos especialistas

Survey response 1

Response ID
1

Date submitted
1980-01-01 00:00:00

Last page
1

Start language
pt

Seed
1140822701

Token
PieEXX0vJNjRRsz

First name
Carlos

Last name
Rabadão

RScB-PT

1 - Partilhar palavras-passe com colegas.

2 - Usar ou criar palavras-passe demasiado simples (ex: nome de familiar, data de nascimento, apelidos, sequencias de carateres, menos de 8 digitos).
Retirava o tamanho. Não é consensual que pwd com mais de 8 caracteres sejam seguras. Aliás, muitas pwd com menos de 8 caracteres são menos fracas do que outras com mais de 8.

3 - Usa a mesma palavra-passe para diferentes websites.

4 - Usa sistemas de armazenamento online para partilhar ou guardar informação pessoal e sensível(google drive, dropbox, onedrive, etc).
A juventude está mais virada para Instagram e outras redes sociais. Quase não sabem o que é google drive, dropbox e onedrive.

5 - Inserir informação de pagamento em jogos “Freemium”, que são gratuitos mas que oferecem benefícios mediante pagamento.
A pergunta original também é relevante. Os jovens também fazem compras online e utilizam plataformas pagas de videojogos. A ideia da pergunta original é se colocam informação sobre meios de pagamentos eletrónicos em todos os sites ou só naqueles "de confiança", seja lá o que isso represente para eles.

6 - Usar redes Wi-Fi de acesso livre (públicas).

7 - Confiar num amigo ou colega próximo para conselhos em aspetos de segurança online.
Confiar nos conselhos de um amigo ou colega próximo sobre em aspetos de segurança online.

8 - Descarregar software antivírus gratuito de fontes desconhecidas.
Muitos jovens já pouco utilizam PC. Usam mais apps em telemóveis e tablets. A questão poderia ser mais generalista ou então abranger mais opções. Tipo instalar aplicações que não a partir das stores oficiais.

9 - Desativar o antivírus do computador para que possa descarregar informação de websites.
Esta seria uma questão candidata a ser substituída por outra mais adequado ao público alvo.

10 - Utilizar a pen drive pessoal com a finalidade de transferir informação para os computadores da escola.

11 - Verificar regularmente as actualizações de software do smartphone/tablet/portátil/PC.

12 - Descarregar conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas.

13 - Partilhar a sua localização nas redes sociais. (Fotos, local de férias...).

14 - Aceitar solicitações de amizade em redes sociais porque reconhece fotos.
pedidos de amizade é um termo mais utilizado.

15 - Clicar em links de email não solicitados de uma fonte desconhecida.
Substituir "links de emails não solicitados" por "links em emails recebidos"

16 - Enviar informação pessoal a estranhos pela Internet (contactos nas redes sociais, darnúmeros de telefone ou email para obter códigos de download ou prémios, etc..).

17 - Clicar em links de email enviados por amigos próximos ou por colegas de trabalho.
de trabalho -> de Escola

18 - Verificar atualizações para quaisquer antivírus que tenha instalado.

19 - Descarregar informação e material de websites para o computador sem verificação da autenticidade.
O termo "autenticidade" é bastante técnico. Avaliar a utilização de outro termo mais utilizado diariamente pelos destinatários do inquérito.

20 - Guardar informação pessoal, de familiares e amigos no dispositivo eletrónico pessoal (por ex., smartphone/tablet/portátil).

Comentários finais e observações:
Recomendo a utilização do termo "Escola" e substituição de "escola".

A.7 AJUSTES NAS ESCALAS RESULTADO DOS CONTRIBUTOS DOS ESPECIALISTAS

A.7.1 *Escala de Atitudes com ajustes sugeridos pelos especialistas*

Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB)	Cybersecurity Attitudes In Schools (CsA-S) Versão final para contexto escolar. (Após validação de especialistas)		
	Original (Inglês)	**Versão final (Inglês)**	**Versão final (Português)**
1	I think that management have the responsibility to ensure a company is protected from cybercrime.	I believe that it is safe to ignore update warnings from computer software.	Acredito que é seguro ignorar avisos de atualizações do software do computador.
2	I am aware of my role in keeping the company protected from potential cybercriminals.	I am aware of my role in keeping the school protected from potential cybercriminals.	Estou ciente do meu papel em manter a escola protegida de potenciais ciberameaças.
3	I believe everyone in the company has a role to play in protecting against threats from cybercriminals.	I believe everyone in the school has a role to play in protecting against threats from cybercriminals.	Penso que todos na escola têm um papel a desempenhar na proteção contra as ciberameaças.
4	It is hard to know how I can help protect the organisation from cybercrime.	It is hard to know how I can help protect the school from cybercrime.	É difícil saber como posso ajudar a proteger a escola do cibercrime.
5	I don't have the right skills to be able to protect the organisation from cybercrime.	I don't have the right skills to be able to protect the school from cybercrime.	Não tenho as competências necessárias para proteger a escola do cibercrime.
6	I do not feel that IT security is a priority within my organisation.	I believe that personal information should not be revealed online, namely who I am, where I live or which school I attend.	Acredito que a informação pessoal não deve ser revelada online, nomeadamente quem sou, onde vivo ou que escola frequento.
7	Computer systems provide all the protection a company needs.	Computer systems provide all the protection a school needs.	Os sistemas informáticos oferecem toda a proteção de que uma escola necessita.
8	I think that reporting cybercrime is a waste of time.	I think that reporting cybercrime is a waste of time.	Creio que denunciar o cibercrime é uma perda de tempo.
9	The Police lack the capacity to deal with cybercrime effectively.	The Police lack the capacity to deal with cybercrime effectively.	As autoridades de segurança não tem meios para combater o cibercrime de forma eficaz.
10	I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.	I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.	Creio que os cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger.
11	I think that information provided by the Government and Police on cybercrime is not relevant to businesses.	I would download copyright material (images, documents, videos).	Faria o download de material abrangido por direitos de autor (imagens, documentos, vídeos).
12	I feel that the Police are far too busy to deal with cybercrime.	I believe when I view violence related content in a school, I may have been promoting its sharing and comments.	Acredito que, quando visualizo conteúdos relacionados com violência em contexto escolar, posso estar a promover a sua partilha e comentários.
13	I worry that if I report a cyberattack to the Police it might damage the reputation of the company	I worry that if I report a cyberattack to the Police it might damage the reputation of the school.	Receio que, se denunciar um ciberataque às autoridades, isso vá prejudicar a reputação da escola.
14	I think more could be done to communicate the risks from cybercrime to individuals in the organisation.	I think more could be done to communicate / disseminate / sensitize the risks from cybercrime to individuals in the school.	Penso que poderá ser feito mais para dar a conhecer/divulgar/sensibilizar os riscos do cibercrime à comunidade educativa.
15	I am aware of the company's IT use policy and attempt to follow it.	I am aware of the schools IT use policy and attempt to follow it.	Estou a par das regras de utilização dos recursos informáticos da Escola e tento segui-la.
16	I would not know how to report a cyberattack if one happened.	I would not know how to report a cyberattack if one happened.	Se ocorrer um ciberataque, não sei/não saberei como denunciá-lo.
17	I don't think that reporting a cyberattack on the company is my responsibility.	I don't think that reporting a cyberattack launched from the school is my responsibility.	Não acho que seja minha responsabilidade denunciar um ciberataque que tenha sido lançado a partir da Escola.
18	I don’t pay attention to company material about the threats from cybercrime.	I don’t pay attention to school material about the threats from cybercrime.	Não presto atenção à informação disponibilizado pela Escola sobre as ameaças do cibercrime.
19	I am confident that I would be able to spot the signs of a cyberattack.	I am confident that I would be able to spot the signs of a cyberattack.	Confio na minha capacidade de detetar/identificar sinais de um ciberataque.
20	I think the biggest threat for IT systems comes from people within the company.	I believe that, when inappropriate content appears online, I should ask for help from an adult.	Acredito que quando aparecem conteúdos inapropriados online, devo pedir ajuda a um adulto.

21	I feel that any individual within the company are at risk of manipulation from confidence tricksters.	I feel that any individual within the school are at risk of manipulation from confidence tricksters.	Sinto que qualquer pessoa da escola está em risco de manipulação por ciber "vigaristas e burlões".
22	I think that cybercriminals only target a company when there is a substantial financial gain.	I think that cybercriminals only target a school when there is a substantial financial gain.	Penso que os cibercriminosos e hackers apenas atingem uma escola quando têm muito a ganhar do ponto de vista financeiro.
23	I believe only large companies are targeted by hackers and cybercriminals.	I believe only companies are targeted by hackers and cybercriminals.	Apenas as grandes empresas e organizações são alvo dos hackers e cibercriminosos.
24	I feel that only companies that take payments using online systems are at risk of being victims of cybercrime.	I feel that only companies that take payments using online systems are at risk of being victims of cybercrime.	Acredito que apenas as instituições que utilizam meios de pagamento online estão em risco de serem vítimas de um ciberataque.
25	I don't think I know who is responsible for protecting the company from cybercrime.	I think that I have the right to be always online, with access to all Internet services.	Penso que tenho o direito de estar sempre online, com acesso a todos os serviços da Internet.

A.7.2 *Escala de Comportamentos com ajustes sugeridos pelos especialistas*

Risky Cybersecurity Behaviours Scale (RScB).	Cybersecurity Behaviors In Schools (CsB-S) Versão final para contexto escolar. (Após validação de especialistas)	

	Original (Inglês)	Versão final (Inglês)	Versão final (Português)
1	Sharing passwords with friends and colleagues.	Sharing passwords with friends and colleagues.	Partilhar palavras-passe com colegas.
2	Using or creating passwords that are not very complicated (e.g. family name and date of birth).	Using or creating passwords that are not very complicated (e.g. family name and date of birth, letter strings).	Usar ou criar palavras-passe demasiado simples. (ex.: nome de familiar, data de nascimento, apelidos, sequencias de carateres)
3	Using the same password for multiple websites.	Using the same password for multiple websites.	Usar a mesma palavra-passe para diferentes websites.
4	Using online storage systems to exchange and keep personal or sensitive information.	Using online storage systems to exchange and keep personal or sensitive information.	Usar sistemas de armazenamento online (cloud) para partilhar ou guardar informação pessoal e sensível.
5	Entering payment information on websites that have no clear security information/certification	Entering payment information on websites that have no clear security information/certification.	Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita.
6	Using free-to-access public Wi-Fi	Using free-to-access public Wi-Fi.	Usar redes Wi-Fi de acesso livre (públicas).
7	Relying on a trusted friend or colleague to advise you on aspects of online-security.	Relying on a trusted friend or colleague to advise you on aspects of online-security.	Confiar nos conselhos de um amigo ou colega próximo sobre aspetos de segurança online.
8	Downloading free anti-virus software from an unknown source.	Downloading free anti-virus software/apps from an unknown source.	Descarregar software/apps antivírus gratuito de fontes desconhecidas.
9	Disabling the anti-virus on my work computer so that I can download information from websites.	Disabling the anti-virus on my computer so that I can download information from websites.	Desativar o antivírus do computador para que possa descarregar informação de websites.
10	Bringing in my own USB to work in order to transfer data onto it.	Bringing in my own USB to school in order to transfer data onto it.	Utilizar a pen drive pessoal com a finalidade de transferir informação para os computadores da Escola.
11	Checking that software for your smartphone/tablet/laptop/PC is up-to-date.	Checking that software for your smartphone/tablet/laptop/PC is up-to-date.	Verificar regularmente as atualizações de software do smartphone/tablet/portátil/PC.
12	Downloading digital media (music, films, games) from unlicensed sources	Downloading digital media (music, films, games) from unlicensed sources.	Descarregar conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas.
13	Sharing my current location on social media.	Sharing my current location on social media.	Partilhar a sua localização nas redes sociais. (Fotos, local de férias...)
14	Accepting friend requests on social media because you recognise the photo.	Accepting friend requests on social media because you recognise the photo.	Aceitar pedidos de amizade em redes sociais porque reconhece fotos.
15	Clicking on links contained in unsolicited emails from an unknown source.	Clicking on links contained in unsolicited emails from an unknown source.	Clicar em links em emails recebidos de uma fonte desconhecida.
16	Sending personal information to strangers over the Internet.	Sending personal information to strangers over the Internet.	Enviar informação pessoal a estranhos pela Internet (contactos nas redes sociais, dar números de telefone ou email para obter códigos de download ou prémios, etc..) .
17	Clicking on links contained in an email from a trusted friend or work colleague.	Clicking on links contained in an email from a trusted friend or colleague.	Clicar em links de email enviados por amigos próximos ou por colegas de Escola.
18	Checking for updates to any anti-virus software you have installed.	Checking for updates to any anti-virus software you have installed.	Verificar atualizações para quaisquer antivírus que tenha instalado.
19	Downloading data and material from websites on my work computer without checking its authenticity.	Downloading data and material from websites on my computer without checking its authenticity.	Descarregar informação e material de websites para o computador sem verificação da veracidade.
20	Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)	Storing personal, family and friends information on my personal electronic device (e.g. smartphone/tablet/laptop).	Guardar informação pessoal, de familiares e amigos no dispositivo eletrónico pessoal. (por ex., smartphone/tablet/portátil)

A.8 QUESTIONÁRIO DE ATITUDES APLICADO EM CONTEXTO ESCOLAR

Atitudes em Relação à Cibersegurança nas Escolas

O meu nome é Frederico Marques, sou atualmente aluno do 2.º ano do Mestrado em Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria.
Estou a trabalhar na dissertação sob orientação do Professor Mário Antunes, que tem como objetivo avaliar o risco dos comportamentos e atitudes dos alunos do ensino básico (6º e 9º anos de escolaridade) face à cibersegurança.
O questionário apresentado é uma versão adaptada para o contexto escolar dos questionários "Attitudes towards cybersecurity and cybercrime in business (ATC-IB)" de Lee Hadlington.

Nesse sentido, solicito a vossa colaboração, respondendo a este questionário que procura identificar padrões de atitudes em Relação à cibersegurança.

As respostas que forem dadas são anónimas e confidenciais, e serão apenas utilizadas no âmbito da realização deste projeto.

Agradeço desde já a vossa disponibilidade e encontro-me disponível para eventuais esclarecimentos que julguem necessários.
(2190377@my.ipleiria.pt)
Existe(m) 29 questão(ões) neste questionário.

Caraterização

Dados dos participantes

Qual o seu género: *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Feminino
- ◯ Masculino

Qual o ano que frequenta: *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 6º. Ano
- ◯ 9º. Ano

Habilitações académicas do Pai: *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Básico (1ºciclo)
- ◯ Básico (2ºciclo)
- ◯ Básico (3ºciclo)
- ◯ Secundário
- ◯ Bacharelato
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento
- ◯ Não sabe

Habilitações académicas do Mãe: *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Básico (1ºciclo)
- ◯ Básico (2ºciclo)
- ◯ Básico (3ºciclo)
- ◯ Secundário
- ◯ Bacharelato
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento
- ◯ Não sabe

Atitudes em Relação à Cibersegurança

Acredito que é seguro ignorar avisos de atualizações do software do computador. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Estou ciente do meu papel em manter a escola protegida de potenciais ciberameaças. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Penso que todos na escola têm um papel a desempenhar na proteção contra as ciberameaças. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

É difícil saber como posso ajudar a proteger a escola do cibercrime. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Não tenho as competências necessárias para proteger a escola do cibercrime. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Acredito que a informação pessoal não deve ser revelada online, nomeadamente quem sou, onde vivo ou que escola frequento. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Os sistemas informáticos oferecem toda a proteção de que uma escola necessita. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Creio que denunciar o cibercrime é uma perda de tempo. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

As autoridades de segurança não tem meios para combater o cibercrime de forma eficaz. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Creio que os cibercriminosos têm conhecimentos mais avançados do que as pessoas que nos deviam proteger. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Faria o download de material abrangido por direitos de autor (imagens, documentos, vídeos). *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Acredito que, quando visualizo conteúdos relacionados com violência em contexto escolar, posso estar a promover a sua partilha e comentários. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Receio que, se denunciar um ciberataque às autoridades, isso vá prejudicar a reputação da escola. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Penso que poderá ser feito mais para dar a conhecer/divulgar/sensibilizar os riscos do cibercrime à comunidade educativa. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Estou a par das regras de utilização dos recursos informáticos da Escola e tento segui-la. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Se ocorrer um ciberataque, não sei/não saberei como denunciá-lo. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Não acho que seja minha responsabilidade denunciar um ciberataque que tenha sido lançado a partir da Escola. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Não presto atenção à informação disponibilizado pela Escola sobre as ameaças do cibercrime. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Confio na minha capacidade de detetar/identificar sinais de um ciberataque. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Acredito que quando aparecem conteúdos inapropriados online, devo pedir ajuda a um adulto. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Sinto que qualquer pessoa da escola está em risco de manipulação por ciber "vigaristas e burlões". *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Penso que os cibercriminosos e hackers apenas atingem uma escola quando têm muito a ganhar do ponto de vista financeiro. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Apenas as grandes empresas e organizações são alvo dos hackers e cibercriminosos. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Acredito que apenas as instituições que utilizam meios de pagamento online estão em risco de serem vítimas de um ciberataque. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Penso que tenho o direito de estar sempre online, com acesso a todos os serviços da Internet. *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Concordo totalmente.
- ◯ Concordo.
- ◯ Discordo.
- ◯ Discordo totalmente.

Obrigado pela sua colaboração!
05.03.2021 – 15:42

Submeter o seu inquérito
Obrigado por ter concluído este inquérito.

A.9 QUESTIONÁRIO DE COMPORTAMENTOS APLICADO EM CONTEXTO ESCOLAR

Comportamentos de Risco em Cibersegurança nas Escolas

O meu nome é Frederico Marques, sou atualmente aluno do 2.º ano do Mestrado em Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria.
Estou a trabalhar na dissertação sob orientação do Professor Mário Antunes, que tem como objetivo avaliar o risco dos comportamentos e atitudes dos alunos do ensino básico (6º e 9º anos de escolaridade) face à cibersegurança.
O questionário apresentado é uma versão adaptada para o contexto escolar dos questionários "Risky cybersecurity behaviours scale (RScB)" de Lee Hadlington.

Nesse sentido, solicito a vossa colaboração, respondendo a este questionário que procura identificar padrões de comportamentos de risco em relação à cibersegurança.

As respostas que forem dadas são anónimas e confidenciais, e serão apenas utilizadas no âmbito da realização deste projeto.

Agradeço desde já a vossa disponibilidade e encontro-me disponível para eventuais esclarecimentos que julguem necessários.
(2190377@my.ipleiria.pt)
Existe(m) 24 questão(ões) neste questionário.

Caraterização

Dados dos participantes

Qual o seu género: *

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Feminino
- ◯ Masculino

Qual o ano que frequenta: *

Escolher uma das seguintes respostas
Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 6º. Ano
- ◯ 9º. Ano

Habilitações académicas do Pai: *

Escolher uma das seguintes respostas
Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Básico (1ºciclo)
- ◯ Básico (2ºciclo)
- ◯ Básico (3ºciclo)
- ◯ Secundário
- ◯ Bacharelato
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento
- ◯ Não sabe

Habilitações académicas do Mãe: *

Escolher uma das seguintes respostas
Por favor, selecione **apenas uma** das seguintes opções:

- ◯ Básico (1ºciclo)
- ◯ Básico (2ºciclo)
- ◯ Básico (3ºciclo)
- ◯ Secundário
- ◯ Bacharelato
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento
- ◯ Não sabe

Comportamentos de risco em cibersegurança

Seleccione a opção que melhor se adapta à frequência com que realiza as ações:
0- Nunca; 1 - 1 a 2 vezes por semestre; 2 -1 a 2 vezes por trimestre; 3 - 1 a 2 vezes por mês; 4 - 1 a 2 vezes por quinzena; 5 - 1 a 2 vezes por semana; 6 - Diariamente

Partilhar palavras-passe com colegas. *

Escolher uma das seguintes respostas
Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Usar ou criar palavras-passe demasiado simples (ex.: nome de familiar, data de nascimento, apelidos, sequencias de carateres). *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Usar a mesma palavra-passe para diferentes websites. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Usar sistemas de armazenamento online (cloud) para partilhar ou guardar informação pessoal e sensível. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Inserir informação de pagamento em websites sem a informação/certificação de segurança explícita. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Usar redes Wi-Fi de acesso livre (públicas). *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Confiar nos conselhos de um amigo ou colega próximo sobre aspetos de segurança online. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Descarregar software/apps antivírus gratuito de fontes desconhecidas. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Desativar o antivírus do computador para que possa descarregar informação de websites. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Utilizar a pen drive pessoal com a finalidade de transferir informação para os computadores da Escola. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Verificar regularmente as atualizações de software do smartphone/tablet/portátil/PC. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Descarregar conteúdos digitais (música, filmes, jogos, etc...) de fontes não fidedignas. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Partilhar a sua localização nas redes sociais (Fotos, local de férias...). *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Aceitar pedidos de amizade em redes sociais porque reconhece fotos. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Clicar em links em emails recebidos de uma fonte desconhecida. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Enviar informação pessoal a estranhos pela Internet (contactos nas redes sociais, dar números de telefone ou email para obter códigos de download ou prémios, etc..) . *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Clicar em links de email enviados por amigos próximos ou por colegas de Escola. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Verificar atualizações para quaisquer antivírus que tenha instalado. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Descarregar informação e material de websites para o computador sem verificação da veracidade. *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Guardar informação pessoal, de familiares e amigos no dispositivo eletrónico pessoal (por ex., smartphone/tablet /portátil). *

Escolher uma das seguintes respostas

Por favor, selecione **apenas uma** das seguintes opções:

- ◯ 0 - Nunca
- ◯ 1 - 1 a 2 vezes por semestre
- ◯ 2 - 1 a 2 vezes por trimestre
- ◯ 3 - 1 a 2 vezes por mês
- ◯ 4 - 1 a 2 vezes por quinzena
- ◯ 5 - 1 a 2 vezes por semana
- ◯ 6 - Diariamente

Obrigado pela sua colaboração!
05.03.2021 – 15:41

Submeter o seu inquérito
Obrigado por ter concluído este inquérito.

A.10 TEXTO DA POLÍTICA DE TRATAMENTO DE DADOS INCLUÍDO NOS QUESTIONÁRIOS

Ao responder a este inquérito, está a prestar de forma livre, consciente e inequívoca o consentimento ao Tratamento de Dados recolhidos, limitando-se a sua utilização à realização da dissertação, com o compromisso de serem tratados em conformidade com O Regulamento Geral de Proteção de Dados (RGPD).
As respostas que forem dadas são anónimas e confidenciais, e serão apenas utilizadas no âmbito da realização deste projeto.
Os dados serão conservados pelo período necessário á realização da dissertação numa base de dados disponibilizada no SurveyMonkey Inc.

Para continuar, primeiro aceite a política de dados. ☑

B

APÊNDICE B - DOCUMENTOS RELACIONADOS COM O QUESTIONÁRIO DE AUTODIAGNÓSTICO

B.1 TAXONOMIA DE REFERÊNCIA PARA CLASSIFICAÇÃO DE INCIDENTES DE SEGURANÇA UTILIZADA

Taxonomia Comum da Rede Nacional de CSIRT

Taxonomia Comum da Rede Nacional de CSIRT

Versão:

3.0

(ENISA / TF-CSIRT RSTI WG v.1002)

Autor:

Grupo de Trabalho - Taxonomia

Revisão:

Grupo de Trabalho - Taxonomia

Janeiro de 2020

Classificação	Data	Versão do documento
TLP:WHITE	Janeiro 2020	3.0

Título
Taxonomia Comum da Rede Nacional de CSIRT

Origem
Rede Nacional de CSIRT – Grupo de Trabalho Taxonomia

Histórico de Versões			
Versão	**Data**	**Revisor**	**Comentários/Notas**
2.5	Dezembro 2012		
3.0	Dezembro 2019	Grupo de Trabalho - Taxonomia	Revisão e Atualização da Taxonomia

ÍNDICE

1 INTRODUÇÃO

Este documento descreve a taxonomia comum para a classificação de incidentes de segurança informática, na Rede Nacional de CSIRT. Esta Taxonomia foi revista durante o ano de 2019 tendo originado a versão 3 deste documento. Como base para esta revisão este Grupo de Trabalho (GT) teve em consideração a Taxonomia de referência do Working Group – RSIT WG[1] [2].

1 https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force
2 https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/reference-security-incident-taxonomy-working-group-2013-rsit-wg

2 CLASSIFICAÇÃO DE INCIDENTES

A classificação de incidentes deverá ser feita de acordo com 2 vetores – "Tipo de Incidente" e "Tipo de Evento". No modelo de classificação de incidentes adotado foi ainda decidida uma divisão dos vários Tipos específicos de incidentes por Classes genéricas que agrupam conjuntos de incidentes com resultados ou objetivos semelhantes. Para além das Classes e Tipos de incidentes, foi ainda identificado um conjunto de eventos associados a cada Tipo de incidente. A tabela seguinte elenca, de forma não exaustiva, os tipos de eventos presentes na taxonomia comum para a Rede Nacional de CSIRT.

Tipo de Evento	**Descrição**
Sistema(s) infetado(s) com malware conhecido	Detetado num sistema a presença de qualquer um dos tipos de malware.
Disseminação de malware através de email	Malware anexado a mensagem ou presença de link para URL malicioso em mensagem de correio eletrónico.
Alojamento de malware em página web	Página web que se encontra a disseminar um dos vários tipos de malware.
Alojamento de servidor de C2	Sistema que é usado como ponto de controlo de uma botnet. Também se inclui neste campo os sistemas que servem como ponto de recolha de dados roubados através de botnets.
Replicação e disseminação de worm	Sistema comprometido com um Worm que tenta comprometer outros sistemas.
Ligação a porto(s) suspeito(s), associado(s) a um determinado malware	Sistema que efectua tentativas de acesso a um porto geralmente associado a um determinado tipo de malware.
Ligação a sistema(s) suspeito(s) associado(s) a um determinado malware	Sistema que efectua tentativas de acesso a um endereço IP ou URL geralmente associado a um determinado tipo de malware como por exemplo - C2 ou página para distribuição de componentes associados a uma determinada botnet.

Flood de pedidos	Envio massivo de pedidos (pacotes de rede, emails, etc.), a partir de uma única fonte, a um determinado serviço com o objectivo de afectar o seu funcionamento.
Exploit ou ferramenta para esgotamento de recursos (rede, capacidade processamento, sessões, etc…)	Utilização, a partir de uma única fonte, de software especialmente concebido para afectar o funcionamento de um determinado serviço através da exploração de uma vulnerabilidade no mesmo.
Flood distribuído de pedidos	Envio massivo de pedidos (pacotes de rede, emails, etc.), a partir de várias fontes, a um determinado serviço com o objectivo de afectar o seu funcionamento.
Exploit ou ferramenta distribuídos para esgotamento de recursos	Utilização, a partir de várias fontes, de software especialmente concebido para afectar o funcionamento de um determinado serviço através da exploração de uma vulnerabilidade no mesmo.
Vandalismo	Actividades lógicas e físicas que não tenham como objectivo premeditado danificar a informação ou evitar a sua transmissão entre sistemas, mas que tenham essa consequência.
Disrupção intencional de mecanismos de transmissão e tratamento de dados	Actividades lógicas e físicas que tenham como objectivo premeditado corromper a informação ou evitar a sua transmissão entre sistemas.
Disrupção não intencional de mecanismos de transmissão e tratamento de dados	Acontecimentos que tenham como consequência não prevista a corrupção da informação ou impossibilidade de transmissão entre sistemas.
Probe a sistema	Scan a um único sistema à procura de portos abertos ou serviços a responderem nesses portos.
Scan de rede	Scan a uma rede de sistemas, com o objectivo de identificar sistemas que estejam activos nessa mesma rede.
Transferência zona DNS	Transferência não autorizada de uma determinada zona de DNS.

Wiretapping	Intercepção lógica ou física de comunicações.
Disseminação de emails de phishing	Envio massivo de emails com o objectivo de recolher dados para efeitos de Phishing das vítimas.
Alojamento de sites de phishing	Alojamento de sites web para efeitos de phishing.
Agregação de informação recolhida em esquemas de phishing	Recolha de dados resultantes de ataques de phishing através de páginas web, contas de correio electrónico, etc…
Tentativa de utilização de exploit	Utilização, sem sucesso, de uma ferramenta que explora uma determinada vulnerabilidade no sistema.
Tentativa de SQL Injection	Tentativa, sem sucesso, de manipulação ou leitura de dados em base de dados, através da técnica de SQL Injection.
Tentativa de XSS	Tentativa, sem sucesso, de ataques recorrendo a técnicas de cross-site scripting.
Tentativa de file inclusion	Tentativa, sem sucesso, de inclusão de ficheiros no sistema alvo através de técnicas de file inclusion.
Tentativa de brute-force	Tentativa de Login, sem sucesso, em sistema através da utilização de credenciais sequenciais de acesso.
Tentativa de password cracking	Tentativa de descoberta de credenciais de acesso através da quebra dos mecanismos criptográficos que os protegem.
Tentativa de ataque dicionário	Tentativa de login, sem sucesso, em sistema através da utilização de credenciais de acesso pré-carregadas em dicionário.
Utilização de exploit local ou remoto	Utilização, com sucesso, de uma ferramenta que explora uma determinada vulnerabilidade no sistema.
SQL Injection	Manipulação ou leitura de dados em base de dados, através da técnica de SQL Injection.
XSS	Ataques recorrendo a técnicas de cross-site scripting.

File inclusion	Inclusão de ficheiros no sistema alvo através de técnicas de file inclusion.
Bypass sistema controlo	Acesso indevido a sistema ou componente contornando um sistema de controlo de acesso existente.
Furto de credenciais de acesso	Acesso indevido a sistema ou componente através da utilização de credenciais de acesso furtadas.
Furto de credenciais de acesso privilegiado	Acesso indevido a sistema ou componente através da utilização de credenciais de acesso privilegiado furtadas.
Acesso indevido e sistema	Acesso não autorizado a um sistema ou componente.
Acesso indevido à informação	Acesso não autorizado a um conjunto de informações.
Exfiltração de dados	Acesso e partilha não autorizados de um determinado conjunto de informações.
Modificação de informação	Alteração indevida de um determinado conjunto de informações.
Eliminação de informação	Eliminação indevida de um determinado conjunto de informações.
Utilização indevida ou não autorizada de recursos	Utilização de recursos da instituição para fins diferentes daqueles para que os mesmos foram afectos.
Utilização ilegítima de nome da instituição ou de terceiros	Utilização de nome da instituição sem autorização da mesma.
Flood de emails	Envio de número anormalmente elevado de mensagens de correio electrónico.
Envio de mensagem não solicitada	Envio de mensagem de correio electrónico não solicitada ou pretendida pelo destinatário.
Distribuição ou partilha de conteúdos protegidos por direitos de autor	Distribuição ou partilha de conteúdos protegidos por direitos de autor e direitos conexos.

Disseminação de conteúdos proibidos por lei (crimes públicos).	Distribuição ou partilha de conteúdos ilegais como pornografia de menores, glorificação da violência, e outros conteúdos proibidos por lei.

Tabela 1 - Classificação de Eventos

Numa fase posterior o incidente deve ser classificado por tipo, segundo a tabela. 2, abaixo.

A ordenação da tabela não reflecte prioridade em casos de múltiplas classificações possíveis para um incidente. A classificação final de um incidente reflectirá a severidade, que poderá variar entre incidentes idênticos, conforme o Membro.

Nesse sentido, e para manter coerência na Rede sobre as estatísticas produzidas, a classificação final de um incidente que envolva mais que um Membro, deverá ser igual entre os Membros envolvidos, devendo o Membro que alterar a classificação, comunicar essa alteração a todos os Membros envolvidos no tratamento desse incidente.

3 TAXONOMIA DE REFERÊNCIA PARA INCIDENTES DE SEGURANÇA [V3.0]

REFERENCE SECURITY INCIDENT TAXONOMY [ENISA V.1002]

Classe de Incidente ***Classification***	**Tipo de Incidente** ***Incident Examples***	**Descrição / Exemplos** ***Description / Examples***
Conteúdo Abusivo *Abusive Content*	Spam *Spam*	Spam ou “email em massa não solicitado”, significa que o destinatário não concedeu permissão verificável para o envio da mensagem e que a mensagem é enviada como parte de uma colecção maior de mensagens, todas com conteúdo funcionalmente comparável. Este IOC refere-se a recursos da infra-estrutura de SPAM, tais como verificadores e/ou colectores de endereços, URL em emails de spam, etc. *Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. This IOC refers to resources, which make up a SPAM infrastructure, be it a harvesters like address verification, URLs in spam e-mails etc.*
	Discurso Nocivo *Harmful Speech*	Individualização ou discriminação de alguém, p. ex. através de ciber perseguição, racismo ou ameaças, contra um ou mais indivíduos. *Discretization or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.*
	Exploração sexual de menores, racismo e apologia da violência *(Child) Sexual Exploitation/Sexual /Violent Content*	Exploração Sexual de Menores, conteúdo sexual, glorificação da violência, e outros conteúdos proibidos por lei. *Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.*

Código Malicioso *Malicious Code*	Sistema Infectado *Infected System*	Sistema infectado com malware, p. ex. PC, smartphone ou servidor infectados com um rootkit. Na maioria das vezes, refere-se a ligações a um servidor C2 “sinkholed”. *System infected with malware, e.g. PC, smartphone or server infected with a rootkit. Most often this refers to a connection to a sinkholed C2 server*
	Servidor C2 *C2 Server*	Servidor de comando e controlo contactado por malware em sistemas infectados. *Command-and-control server contacted by malware on infected systems.*
	Distribuição de Malware *Malware Distribution*	URI usado para distribuição de malware, p. ex. um URL para download, incluído em factura falsa, distribuída via spam de malware. *URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.*
	Configuração de Malware *Malware Configuration*	URI de alojamento de ficheiro de configuração de malware, p. ex. código web para injecção de trojans bancários. *URI hosting a malware configuration file, e.g. web-injects for a banking trojan.*
Recolha de Informação *Information Gathering*	Scanning *Scanning*	Ataques baseados em pedidos realizados a um sistema com o intuito de descobrir pontos fracos. Também inclui processos de teste para recolha de informações sobre sistemas, serviços e contas. Exemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT, etc.), scanning de portos. *Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.*
	Sniffing *Sniffing*	Observação e/ou gravação de tráfego de rede (intercepção). *Observing and recording of network traffic (wiretapping).*

	Engenharia Social *Social Engineering*	Recolha de informações de um ser humano através de meios não técnicos (por exemplo, mentiras, truques, subornos ou ameaças). *Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).*
Tentativa de Intrusão *Intrusion Attempts*	Exploração de Vulnerabilidade *Exploitation of known Vulnerabilities*	Tentativa de comprometer um sistema ou corromper um serviço, através da exploração de vulnerabilidades com um identificador padronizado, como o CVE (p. ex.: "buffer overflow", "backdoor", "cross site scripting", etc.) *An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.)*
	Tentativa de *login* *Login attempts*	Múltiplas tentativas de login (adivinha, quebra ou *bruteforcing* de passwords). Este IOC refere-se a um recurso que foi observado a executar um ataque de força bruta sobre um determinado protocolo aplicacional. *Multiple login attempts (Guessing / cracking of passwords, brute force). This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol.*
	Nova assinatura de ataque *New attack signature*	Ataque que usa a exploração de uma vulnerabilidade desconhecida. *An attack using an unknown exploit.*
Intrusão *Intrusions*	Compromisso de Conta Privilegiada *Privileged Account Compromise*	Compromisso de um sistema em que o atacante ganhou privilégios de administração. *Compromise of a system where the attacker gained administrative privileges.*
	Compromisso de Conta Não Privilegiada *Unprivileged Account Compromise*	Compromisso de um sistema usando uma conta não privilegiada (utilizador/serviço). *Compromise of a system using an unprivileged (user/service) account.*

	Compromisso de Aplicação *Application Compromise*	Compromisso de uma aplicação/software através de vulnerabilidades (des)conhecidas, p. ex. *SQL injection*. *Compromise of an application by exploiting (un-)known software vulnerabilities, e.g. SQL injection.*
	Arrombamento *Burglary*	Intrusão física, p. ex. no edifício da entidade ou no datacenter. *Physical intrusion, e.g. into corporate building or data-centre.*
Disponibilidade *Availability*	Negação de Serviço *Denial of Service*	Ataque de Negação de Serviço, p. ex. envio de pedidos para uma aplicação web, especialmente concebidos para provocarem falha ou lentidão. *Denial of Service attack, e.g. sending specially crafted requests to a web application which causes the application to crash or slow down.*
	Negação de Serviço Distribuída *Distributed Denial of Service*	Ataque distribuído de negação de serviço, p. ex. *SYN-Flood* ou ataques de reflexão/amplificação. *Distributed Denial of Service attack, e.g. SYN-Flood or UDP-based reflection/amplification attacks.*
	Configuração incorreta *Misconfiguration*	Configuração incorrecta de software que resulta em problemas de disponibilidade de serviço, p. ex. um servidor DNS com a DNSSEC KSK da zona raiz, desactualizada. *Software misconfiguration resulting in service availability issues, e.g. DNS server with outdated DNSSEC Root Zone KSK.*
	Sabotagem *Sabotage*	Sabotagem física, p. ex. corte de cabos ou fogo posto. *Physical sabotage, e.g cutting wires or malicious arson.*
	Interrupção *Outage*	Interrupção provocada p. ex. por falha de ar condicionado ou desastre natural. *Outage caused e.g. by air condition failure or natural disaster.*

Segurança da Informação *Information Content Security*	Acesso não autorizado *Unauthorised access to information*	Acesso não autorizado à informação, p. ex. o abuso de credenciais roubadas para acesso a um sistema ou aplicação, intercepção de tráfego ou obtenção de acesso a documentos físicos. *Unauthorised access to information, e.g. by abusing stolen login credentials for a system or application, intercepting traffic or gaining access to physical documents.*
	Modificação não autorizada *Unauthorised modification of information*	Modificação não autorizada de informação, p. ex. um atacante usar credenciais roubadas para acesso a um sistema ou aplicação, ou a encriptação de dados resultante de *ransomware*. *Unauthorised modification of information, e.g. by an attacker abusing stolen login credentials for a system or application or a ransomware encrypting data.*
	Perda de dados *Data Loss*	Perda de dados, p. ex. falha de disco rígido ou furto/roubo. *Loss of data, e.g. caused by harddisk failure or physical theft.*
Fraude *Fraud*	Utilização indevida ou não autorizada de recursos *Unauthorised use of resources*	Utilização de recursos da instituição para fins diferentes daqueles para que os mesmos foram afectos, incluindo para fins lucrativos, p. ex. o uso de e-mail para participar na obtenção de lucros ilegais através de correntes de e-mails ou esquemas de pirâmide. *Using resources for unauthorised purposes including profit-making ventures, e.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes.*
	Direitos de autor *Copyright*	Distribuição ou instalação de software comercial não licenciado ou outros conteúdos protegidos por direitos de autor (Warez). *Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).*

	Utilização ilegítima de nome de terceiros *Masquerade*	Tipo de ataque no qual uma entidade usa ilegalmente a identidade de outra para seu benefício. *Type of attack in which one entity illegitimately impersonates the identity of another in order to benefit from it.*
	Phishing *Phishing*	Entidade que se tenta passar por outra de modo a persuadir o utilizador a revelar credenciais privadas. Este IOC normalmente é um URL usado para phishing de credenciais do utilizador. *Masquerading as another entity in order to persuade the user to reveal private credentials. This IOC most often refers to a URL, which is used to phish user credentials.*
Vulnerabilidade *Vulnerable*	Criptografia fraca *Weak crypto*	Serviços publicamente acessíveis permitindo criptografia fraca, p. ex. servidores web susceptíveis a ataques POODLE/FREAK. *Publicly accessible services offering weak crypto, e.g. web servers susceptible to POODLE/FREAK attacks.*
	Amplificador DDoS *DDoS amplifier*	Serviços publicamente acessíveis, passíveis de serem abusados para ataques DDoS de reflexão/amplificação, p. ex. open-resolvers DNS e servidores NTP com “monlist” activo. *Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks, e.g. DNS open-resolvers or NTP servers with monlist enabled.*
	Serviços acessíveis potencialmente indesejados *Potentially unwanted accessible services*	Serviços publicamente acessíveis eventualmente indesejados, p. ex. Telnet, RDP ou VNC. *Potentially unwanted publicly accessible services, e.g. Telnet, RDP or VNC.*
	Revelação de informação *Information disclosure*	Serviços publicamente acessíveis eventualmente revelando informação sensível, p. ex. SNMP ou Redis. *Publicly accessible services potentially disclosing sensitive information, e.g. SNMP or Redis.*

	Sistema vulnerável *Vulnerable system*	Um sistema vulnerável a certos ataques, p. ex.: má configuração de definições de cliente proxy (ex.: WPAD), sistemas operativos desactualizados, etc. *A system which is vulnerable to certain attacks. Example: misconfigured client proxy settings (example: WPAD), outdated operating system version, etc.*
Outro *Other*	Sem tipo *Uncategorised*	Todos os incidentes que não se encaixam num dos tipos especificados devem ser colocados nesta classe, ou o incidente não é classificado. *All incidents which don't fit in one of the given categories should be put into this class or the incident is not categorised.*
	Indeterminado *Undetermined*	A classificação do incidente é desconhecida/indeterminada. *The categorisation of the incident is unknown/undetermined.*
Teste *Test*	Teste *Test*	Destinado a testes *Meant for testing.*

Tabela 2 - Classificação de Incidentes

4 CORRELAÇÃO ENTRE EVENTOS E INCIDENTES

Porque poderá ser necessário aplicar mecanismos de classificação automática de incidentes, sugere-se como referência o seguinte modelo relacional entre "Tipo de Evento" e "Tipo de Incidente". Importa, no entanto, que esta associação não é estrita, podendo um determinado Tipo de Evento estar associado a qualquer Tipo de Incidente.

Tipo de Evento	**Tipo Incidente**	**Classe de Incidente**
Flood de emails	SPAM	Conteúdo Abusivo
Envio de mensagem não solicitada		
Publicação de informação com o objectivo de intimidar ou coagir outrem	Discurso Nocivo	
Disseminação de conteúdos proibidos por lei (crimes públicos)	Exploração sexual de menores, racismo e apologia da violência	
Sistema(s) ou software(s) infectado(s) com malware permitindo acesso remoto, monitorização de actividades do sistema e recolha de informações	Sistema Infectado	Código Malicioso
Alojamento de servidor C2	Servidor C2	
Disseminação de malware através de vários canais de comunicação	Distribuição de Malware	
Probe a sistema	Scanning	Recolha de Informação
Scan de rede		
Transferência zona DNS		
Wiretapping	Sniffing	

Informação obtida através de meios não técnicos passível de ser usada em ataques futuros	Engenharia Social	
Tentativa de utilização de exploit	Exploração de Vulnerabilidade	Tentativa de Intrusão
Tentativa de SQL Injection		
Tentativa de XSS		
Tentativa de File Inclusion		
Tentativa de Brute-force	Tentativa de *login*	
Tentativa de password cracking		
Tentativa de Ataque Dicionário		
Furto de credenciais de acesso privilegiado	Compromisso de Conta Privilegiada	Intrusão
Furto de credenciais de acesso	Compromisso de Conta Não Privilegiada	
Entrada não autorizada em instalações físicas	Arrombamento	
Exploit ou ferramenta para esgotamento de recursos (rede, capacidade processamento, sessões, etc…)	Negação de Serviço	Disponibilidade
Flood de pedidos		
Flood distribuído de pedidos	Negação de Serviço Distribuída	
Exploit ou ferramenta distribuídos para esgotamento de recursos		
Vandalismo	Sabotagem	
Disrupção intencional de mecanismos de transmissão e tratamento de dados.		
Disrupção não intencional de mecanismos de transmissão e tratamento de dados	Interrupção	

Acesso indevido e sistema	Acesso não autorizado	Segurança da Informação
Acesso indevido à informação		
Exfiltração de dados		
Modificação de informação	Modificação não autorizada	
Eliminação de informação	Perda de dados	
Utilização indevida ou não autorizada de recursos	Utilização indevida ou não autorizada de recursos	Fraude
Distribuição ou partilha de conteúdos protegidos por direitos de autor	Direitos de autor	
Utilização ilegítima de nome da instituição ou de terceiros	Utilização ilegítima de nome de terceiros	
Disseminação de emails de phishing	Phishing	
Alojamento de sites de phishing		
Agregação de informação recolhida em esquemas de phishing		
Utilização de mecanismos de cifra considerados inseguros	Criptografia fraca	Vulnerabilidade
Servidor NTP configurado com *monlist*	Amplificador DDoS	
RDP exposto	Serviços acessíveis potencialmente indesejados	
Documentos internos acessíveis em partilha pública	Revelação de Informação	

Sistema sem actualizações/correcções de segurança.	Sistema vulnerável	

Tabela 3 - Relação não exaustiva entre Tipos de Evento e Tipos de Incidente

5 LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

- C2 - Command and Control
- CNCS - Centro Nacional de Cibersegurança
- CSIRT - Computer Security Incident Response Team
- DDoS - Distributed Denial of Service
- DNSSEC - Domain Name System Security Extensions
- IOC - Indicator of compromise
- KSK - Key signing key
- NTP - Network Time Protocol
- OS - Operating System
- RDP - Remote Desktop Protocol
- SIEM - Security Information and Event Management
- SMTP - Simple Mail Transfer Protocol
- SNMP - Simple Network Management Protocol
- SOC - Security Operations Center
- SPAM - Sending and Posting Advertisement in Mass
- SSH - Secure Shell
- SSL - Secure Sockets Layer
- URI - Uniform Resource Identifier
- URL - Uniform Resource Locator
- VNC - Virtual Network Computing
- VPN - Virtual Private Network
- WPAD - Web Proxy Autodiscovery Protocol

6 LISTA DE TERMOS

- Evento - ocorrência identificável, com um efeito potencialmente adverso na segurança das redes e dos sistemas de informação
- Incidente - um evento com um efeito adverso real na segurança das redes e dos sistemas de informação.
- Log - um registo da actividade que ocorre nos sistemas de informação e comunicação, de uma organização.
- Malware - software ou firmware destinado a executar um processo não autorizado que terá um impacto adverso na confidencialidade, integridade ou disponibilidade de um sistema de informação
- Monlist - comando que permite recolher informação de monitorização de tráfego do serviço NTP
- Proxy - software que recebe um pacote de rede de um cliente e envia o mesmo em nome do cliente para o destino desejado
- Syslog - um protocolo que especifica um formato geral de introdução e um mecanismo de transporte de logs
- Timestamp - uma sequência de caracteres ou informações codificadas que identificam quando um determinado evento ocorreu, fornecendo geralmente a data, a hora do dia, e por vezes são precisas até à fracção de segundo
- Warez - termo cultural global referente a software pirateado que é distribuído pela Internet

7 AGRADECIMENTOS

Esta revisão da Taxonomia Comum da Rede Nacional de CSIRT, é resultado dos trabalhos desenvolvidos pelo Grupo de Trabalho da Taxonomia (GT) instituído pela Rede para a revisão da taxonomia. Elaborado com base num documento prévio, importa atribuir os devidos agradecimentos aos autores desse documento e de outros que eventualmente lhes tenham antecedido.

É também reconhecida a disponibilidade dos Membros do GT, que através do empenho dos seus representantes, permitiram incorporar valiosos contributos nos trabalhos e atingir os resultados propostos com sucesso. O GT, à data deste documento, era constituído pelos Membros (por ordem alfabética):

- Coordenação
  - CSIRT.UMINHO
- Membros
  - CERT.PT
  - CSIRT.UA
  - CSIRT.UPORTO
  - CSIRT.UTAD
  - CSIRT-EY
  - DGS-IRT
  - EDP CSIRT
  - Euronext CSIRT
  - LAYER8 CSIRT
  - RCTS CERT
- Observadores
  - PJ UNC3T

B.2 PERGUNTAS INCLUÍDAS NO QUESTIONÁRIO DE AUTODIAGNÓSTICO

Perguntas do questionário de autodiagnóstico

Classificação de incidentes segundo a

Taxonomia Comum da Rede Nacional de CSIRT (v3.0)

Índice

Código Malicioso

Sistema Infetado

Pergunta: Quais dos seguintes são sinais de que o seu sistema está infetado com vírus?

1 – O antivírus deixou de funcionar.

2 – Mensagens estranhas aparecem no ecrã.

3 – O seu computador ficar muito lento.

4 – Todas as opções anteriores.

Sugestão de leitura:

O antivírus deixar de funcionar é das primeiras ações que um vírus pode provocar num computador, é recomendado tentar ligar imediatamente o antivírus ou até instalar um novo.

Outro sinal de alerta, é a presença de mensagens estranhas no ecrã, podendo ser do antivírus a detetar a presença de vírus ou até mesmo do próprio software malicioso.

Caso o computador fique muito lento, aqueça muito e reinicie regularmente sem qualquer aviso, também pode ser um sintoma de um sistema infetado.

Link de leitura sugerido:

https://www.deco.proteste.pt/tecnologia/antivirus/dicas/6-sinais-de-que-o-seu-computador-esta-infetado-com-virus

Pergunta: Como evitar que o teu computador seja infetado com vírus ou *malware*?

1 – Utilização prudente.

2 – Descarregar conteúdos, só depois de instalar um antivírus.

3 – Não abrir anexos.

4 – Todas as opções anteriores.

Sugestão de leitura:

Utilizar o computador de forma prudente, descarregar conteúdos e anexos apenas posteriormente a instalação de um antivírus, são práticas que ajudam o seu sistema a estar seguro.

Caso necessite de abrir anexos verifique sempre a sua origem, considerando que mesmo com antivírus a sua abertura pode comprometer a sua segurança.

Link de leitura sugerido:

https://www.deco.proteste.pt/tecnologia/antivirus/dicas/6-sinais-de-que-o-seu-computador-esta-infetado-com-virus

Pergunta: Qual dos seguintes podem ser sinais de que o seu sistema está infetado com vírus?

1 – Constante aparecimento de pop-ups, barras de ferramentas indesejadas, substituição da página de entrada.

2 – Acesso web muito lento e o ventilador do PC em funcionamento de forma persistente.

3 – Se os seus contactos de e-mail disserem que recebem spam ou mensagens infetadas do seu endereço.

4 – Todas as opções anteriores.

Sugestão de leitura:

O aparecimento de mensagens estranhas no ecrã, muito tráfego de rede, acesso á internet muito lento e as ventoinhas do PC constantemente a funcionar ou se os seus contactos de e-mail disserem que recebem spam ou mensagens infetadas do teu endereço, são normalmente sinais de alerta que podem indiciar que o equipamento está infetado com vírus.

Link de leitura sugerido:

https://www.deco.proteste.pt/tecnologia/antivirus/dicas/6-sinais-de-que-o-seu-computador-esta-infetado-com-virus

Distribuição de Malware

Pergunta: Qual das seguintes é uma forma de distribuição de malware?

1 – Emails de *phishing*.

2 – Explorando vulnerabilidades do software, e/ou pela instalação de software ilegal.

3 – Através de ataques *drive-by-download*, que explora as vulnerabilidades do navegador para carregar o código malicioso.

4 – Todas as opções anteriores.

Sugestão de leitura:

O *malware* é um dos grandes problemas de cibersegurança da atualidade, e a sua distribuição sendo a sua distribuição atualmente feita por emails de *phishing*, explorando vulnerabilidades do software, pela instalação de software ilegal e através de ataques *drive-by-download*, que explora as vulnerabilidades do navegador para carregar o código malicioso.

A proteção passa por:

- Confirmar sempre se os endereços de e-mail e o url dos websites são os verdadeiros, caso sejam fontes desconhecidas, nunca entrar no website nem descarregar ficheiros em anexo do e-mail.
- Manter sempre o sistema operativo atualizado, pois podem ser encontradas a qualquer momento vulnerabilidades de software e serem lançadas novas atualizações para solucionar o problema.
- Transferir apenas aplicativos de sites confiáveis, de preferência, sempre do site oficial do produto.

Link de leitura sugerido:

https://www.avg.com/pt/signal/what-is-adware

https://pt.malwarebytes.com/malware/

Pergunta: Qual é a melhor forma de definir o que é um ataque de *ransomware*?

1 – Um código malicioso, desenvolvido para causar danos em computadores e servidores.

2 – Código malicioso que recolhe dados do teu equipamento sem o teu conhecimento.

3 – Código malicioso que impede o acesso aos teus ficheiros e dados até que um resgate seja pago.

4 – Código malicioso que tem a capacidade de se auto-replicar, com o intuito de causar a perda ou alteração da informação.

Sugestão de leitura:

Um ataque de *ransomware*, tem origem em software malicioso que encripta os dados do computador de forma a que a vítima não o consiga utilizar, e exigindo um pagamento para que o sistema e os dados voltem a estar disponíveis. Este tipo de ataque, normalmente tem origem em esquemas de *phishing*.

Link de leitura sugerido:

https://www.cncs.gov.pt/queres-ter-os-teus-ficheiros-entao-paga/

https://br.malwarebytes.com/ransomware/

https://www.cncs.gov.pt/recursos/glossario/

Pergunta: Qual das seguintes opções pode levar à disseminação de um programa malicioso?

1 – Manter o antivírus atualizado.

2 – Utilizar apenas software que foi verificado para a presença de vírus.

3 – Utilizar um dispositivo USB de uma fonte desconhecida para trocar dados.

4 - Abrir apenas anexos onde foi verificada a presença de vírus e de fontes conhecidas.

Sugestões de leitura:

Um "Programa malicioso" é qualquer software concebido para danificar um computador. Os programas maliciosos podem roubar informações confidenciais do seu computador, fazê-lo abrandar gradualmente. Formas comuns de distribuição são os dispositivos USB, e websites infetados e emails.

Link de leitura sugerido:

https://pt.malwarebytes.com/malware/

Pergunta: Qual das ações pode prevenir ataque de *Malware* e *Ransomware*?

1 – Utilizar antivírus.

2 – Usar uma Firewall.

3 – Instalar as atualizações de segurança mais recentes.

4 – Todas as opções anteriores.

Sugestão de leitura:

Quanto mais medidas de segurança forem adotadas melhor. A utilização de um antivírus e firewall é recomendada, mas também é muito importante corrigir as vulnerabilidades conhecidas do software e as atualizações de segurança logo que são disponibilizadas.

É também recomendada a criação de copias de segurança, garantindo a possibilidade de recuperação de um ataque deste tipo quando as medidas anteriores falharem.

Link de leitura sugerido:

https://www.kaspersky.com.br/resource-center/threats/how-to-prevent-ransomware

https://br.malwarebytes.com/ransomware/

Servidor C2(servidor de comando e controlo)

Pergunta: Completa a frase para que seja falsa.

Um equipamento controlado por um servidor de comando e controlo (Servidor C2) ….

1 – não está infetado por *malware*.

2 – não permite o acesso aos dados nele armazenados.

3 – pode desligar ou reiniciar o servidor.

4 – pode ser utilizada para ataques de Negação de serviço distribuída (DDoS).

Sugestão de leitura:

Um servidor de comando e controlo (Servidor C2) é um computador que dá ordens a aparelhos infetados por um *malware* e que recebe informação desses aparelhos.

Link de leitura sugerido:

https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server

Configuração de Malware

Pergunta: Quando os criminosos conseguem aceder ao computador de alguém e encriptam os dados e ficheiros. O utilizador não consegue aceder aos seus dados se não pagar aos criminosos para os desencriptar. A isto chama-se?

1 – Botnet.

2 – Spam.

3 – Ransomware.

4 – Nenhuma das opções anteriores.

Sugestão de leitura:

Ransomware é um programa com objetivos maliciosos que infecta o computador da vítima e o bloqueia ou deixa o seu conteúdo criptografado, e exige pagamentos para se colocar o sistema novamente a funcionar.

Link de leitura sugerido:

https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware

Disponibilidade

Negação de Serviço

Pergunta: O que é um ataque de negação de serviço (DoS)?

1 – Ataque de rede que permite a um hacker desligar remotamente um computador.

2 – Uma ferramenta que impede hackers de usarem os serviços de rede.

3 – Qualquer ataque que pretenda impedir os utilizadores de usar recursos digitais.

4 –Um computador utilizado para atacar hacker.

Sugestão de leitura:

Um ataque de negação de serviço (DoS), é um ataque que provoca uma sobrecarga nos equipamentos, normalmente pelo envio de pacotes em larga escala, afeta servidores (mas não só), e faz com que o alvo do ataque fique muito lento ou fique indisponível para os seus utilizadores.

Link de leitura sugerido:

https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/

Negação de Serviço Distribuída

Pergunta: Quais os serviços das empresas que podem ser visados pelos ataques DDoS?

1 – Websites públicos e portais destinados a clientes.

2 – Servidores de correio e mensagens.

3 – Servidores de ficheiros.

4 – Todas as opções anteriores.

Sugestão de leitura:

Um criminoso que realiza um ataque de DDoS pode usar como vítima qualquer um dos serviços disponibilizados pelas empresas. Aproveita os limites de capacidade de todos os recursos de rede, enviando múltiplas solicitações de um recurso invadido com o objetivo de exceder a capacidade que tem de lidar com diversas solicitações. Um ataque DDoS pode ser realizado com milhões de computadores, enquanto um ataque de DoS apenas envolve um atacante.

Link de leitura sugerido:

https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/

https://www.kaspersky.com.br/resource-center/threats/ddos-attacks

https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/

Configuração incorreta

Pergunta: A configuração incorreta de software pode estar na origem de problemas de segurança.

Qual dos seguintes é considerado um problema de configuração incorreta:

1 – Criação de regras de firewall pelos utilizadores.

2 – Antivírus desatualizado ou com licença expirada.

3 – Equipamentos com configurações por omissão.

4 – Todas as opções anteriores.

Sugestão de leitura:

A configuração de software com valores por omissão ou com configurações incorretas representa um risco de segurança, pois são uma porta de entrada para a rede, sendo as configurações incorretas utilizadas pelos invasores para criar Worm e outros tipos de *malware* direcionados.

Link de leitura sugerido:

https://www.manageengine.com/vulnerability-management/misconfiguration/

Sabotagem

Pergunta: Que medidas podes tomar com o objetivo de proteger o teu hardware e software de ações de sabotagem?

1 – Instalar e manter uma firewall e software antivírus.

2 – Disponibilizar utilizadores separados para cada pessoa que usa o computador.

3 – Utilizar perfis de utilizador com permissões limitadas.

4 – Todas as opções anteriores.

Sugestão de leitura:

A sabotagem de hardware consiste em ataques com intenção de desativar computadores ou redes com o objetivo de interromper os serviços disponibilizados pelas instituições, cometer espionagem ou facilitar conspirações criminosas.

Atos simples como, infetar deliberadamente um computador com um vírus para impedir que utilizadores autorizados façam login. Pode também passar pelo uso de *malware*, como *bots*, *worms*, vírus e outros *spywares*, o que permite que hackers obtenham acesso ilegal a computadores pessoais e corporativos.

A proteção passa por instalar e manter uma firewall e software antivírus, estabeleça IDs de Utilizador separadas para cada pessoa que usa um computador com permissões limitadas.

Link de leitura sugerido:

https://www.reference.com/world-view/computer-sabotage-26aedb2d35d843eb

Pergunta: A sabotagem de computadores:

1 – acontece por ação deliberada de um utilizador.

2 – pode envolver o uso de malware, como bots, worms, vírus e outros spywares.

3 – pode passar por permitir o acesso indevido aos equipamentos ou eliminar informação.

4 – Todas as opções anteriores.

Sugestão de leitura:

Atos simples como, infetar deliberadamente um computador com um vírus para impedir que utilizadores autorizados façam login. Pode também passar pelo uso de *malware*, como *bots*, *worms*, vírus e outros *spywares*, o que permite que hackers obtenham acesso ilegal a computadores pessoais e corporativos.

A proteção passa por instalar e manter uma firewall e software antivírus, estabeleça IDs de Utilizador separadas para cada pessoa que usa um computador com permissões limitadas.

Link de leitura sugerido:

https://www.reference.com/world-view/computer-sabotage-26aedb2d35d843eb

Interrupção

Pergunta: Uma falha de sistema (Interrupção) pode ser provocada por desastres naturais, avarias de hardware, utilizadores mal-intencionado entre outros.

Como se pode mitigar (minimizar) este tipo de problemas:

1 – Criar e verificar regulamente backups.

2 – Imprimir os dados armazenados.

3 – Restringir o acesso a utilizadores autorizados.

4 – Todas as opções anteriores.

Sugestão de leitura:

Um ataque de interrupção, provoca a degradação ou torna indisponível para uso legítimo os recursos, pode ter origem num ataque, desastres naturais, avarias de hardware, utilizadores mal-intencionados ou outros.

A criação e verificação regular de backups é sem dúvida uma das formas mais seguras de garantir a proteção e salvaguarda de toda a informação.

O procedimento não é muito complexo, e pretende guardar uma cópia de toda a informação que possa ser utilizada/recuperada quando necessário. Os backups podem ser integrais ou incrementais, sendo os integrais uma copia nova e completa de toda a informação e as incrementais, cópias com a informação que vai sendo modificada.

Link de leitura sugerido:

https://www.cncs.gov.pt/newsletters/newsletter-n5/o-que-e-um-backup/

https://br.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html

https://br.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html

Recolha de Informação

Scanning

Pergunta: Um ataque de Scanning consiste em:

1 – Enviar mensagens para portas do sistema analisado e esperar por uma resposta.

2 – Identificar portos e serviços disponíveis no sistema a ser analisado.

3 – Recolher informação de um sistema e identificar vulnerabilidades conhecidas.

4 – Todas as opções anteriores.

Sugestão de leitura:

Um ataque de *Scanning* consiste no envio de mensagens para o sistema a ser analisado e esperar por uma respostas, identificando portos e serviços disponíveis, e que pode ser utilizado para identificar vulnerabilidades conhecidas.

Pode também revelar a presença de medidas de segurança em vigor, sendo comum preceder os ataques propriamente ditos.

Link de leitura sugerido:

https://www.avast.com/pt-pt/business/resources/what-is-port-scanning

https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/

Sniffing

Pergunta: Que tipo de risco pode ser minimizado utilizando uma Virtual Private Network (VPN)?

1 – Impedir a exposição e disponibilização de informações quando estás ligado a redes Wi-Fi de acesso livre (públicas).

2 – Impedir a utilização de keyloggers (gravar/registar as teclas pressionadas num teclado).

3 – Impedir ataques de Engenharia Social.

4 – Impedir ataques de Phishing.

Sugestão de leitura:

Uma VPN, oferece privacidade online, impedindo a exposição e disponibilização de informações, dos utilizadores.

Link de leitura sugerido:

https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

Pergunta: O que significa "https: //" no início de um URL, em oposição a "http: //"?

1 - Identifica uma ligação segura a um servidor, encriptando os dados trocados.

2 - Identifica um website na sua última versão, que não encripta dados.

3 – Identifica um website que recolhe dados dos utilizadores.

4 – Nenhuma das opções anteriores.

Sugestão de leitura:

No mundo atual, os dados têm grande valor, por isso devemos ser muito cuidadosos e verificar se as informações que partilhamos são transmitidas por uma conexão segura. (HTTPS)

Um url que inicia com HTTPS identifica uma ligação segura com um servidor, protegendo assim os dados, com a ajuda de um certificado SSL válido.

Link de leitura sugerido:

https://nordvpn.com/pt/blog/http-ou-https/

Engenharia Social

Pergunta: Qual das afirmações é verdadeira quando se fala de ataques de engenharia social?

1 – Utilizam a manipulação emocional dos utilizadores.

2 – O objetivo pode ser interromper ou corromper dados para causar danos.

3 – O objetivo pode ser a obtenção de objetos de valor como informações, acesso ou dinheiro.

4 – Todas as opções anteriores.

Sugestão de leitura:

Designa-se por engenharia social, o processo de tentar convencer alguém de algo fictício, usando interações que podem assumir várias formas: mensagens de correio eletrónico, interações através das redes sociais ou mesmo chamadas telefónicas.

É atualmente, considerada um dos maiores riscos de segurança das pessoas e das organizações. As técnicas de ataque são cada vez mais sofisticadas e a vítima muitas vezes não tem a devida noção do ataque.

Link de leitura sugerido:

https://www.cncs.gov.pt/engenharia-social/

https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

Pergunta: Dos seguintes, qual não é, um ataque de engenharia social?

1 – Email phishing.

2 – vishing (Phishing de voz).

3 – smishing (SMS phishing).

4 – Port Scanning Attack.

Sugestão de leitura:

A engenharia social é uma técnica de manipulação que explora o erro humano para obter informações privadas, acesso ou objetos de valor. No cibercrime, este tipo de golpe tende a atrair utilizadores menos conscientes para que exponham dados, espalhem infeções por *malware* ou forneçam acesso a sistemas de acesso restrito.

Link de leitura sugerido:

https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering
https://www.cncs.gov.pt/engenharia-social/

Intrusão

Compromisso de Conta Privilegiada

Pergunta: Como podes melhorar a tua segurança online?

1 – Utilizar autenticação de duas etapas para aceder às tuas suas contas.

2 – Configurar alertas, para que cada vez que se acede de um novo dispositivo a uma conta, sejas notificado.

3 – Utilizar palavras pass exclusivas para cada conta online e atualizá-las periodicamente.

4 – Todas as opções anteriores.

Sugestões de leitura:

Uma das formas mais simples de se roubar informação é através da obtenção de um conjunto de combinações de passwords e logins e tentar utilizá-las em vários serviços diferentes.

A forma mais simples de evitar que um roube de informação se multiplique por vários sites é ter uma password diferente em cada um deles.

Com a verificação em duas etapas, também conhecida como autenticação de dois fatores, é adicionada uma camada extra de segurança caso a senha seja roubada. Com a verificação em duas etapas ativa, o login na conta é feito com algo que se sabe (como sua senha), e algo que se tem (como o telemóvel).

A configuração de alertas também pode ajudar a aumentar o nível de segurança pois permite que cada vez que um novo dispositivo aceda a uma conta o utilizador seja notificado.

Link de leitura sugerido:

https://www.cncs.gov.pt/content/files/bp_pp_nov19.pdf

https://www.cncs.gov.pt/content/files/password.pdf

Pergunta: Completa a frase seguinte, para que esteja correta:

O uso de uma conta de administrador para executar tarefas diárias …….

1 - é recomendado porque ajudar a proteger o PC.

2 – não é recomendado porque pode resultar em danos significativos e/ou comprometimento da segurança do seu sistema.

3 – é recomendado porque dá a liberdade de instalar ou desinstalar software no computador.

4 – é preferível comparativamente com outros tipos de utilizadores porque permite o acesso à maioria dos programas, mas sem a possibilidade de fazer alterações.

Sugestões de leitura:

As contas de administrador permitem fazer qualquer tipo de mudanças no computador, o que pode ser um grande problema de segurança.

A melhor maneira de manter o computador seguro é ter duas contas: uma de administrador e uma de utilizador comum. A conta de administrador, deverá ser usada quando for necessário instalar ou desinstalar programas, ou para qualquer outra atividade avançada. A outra conta (utilizador comum) não terá este tipo de permissões e deverá ser usada de diariamente.

Link de leitura sugerido:

https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management

Compromisso de Conta Não Privilegiada

Pergunta: Das afirmações seguintes, qual justifica, porque se deve fazer sempre login num equipamento com utilizador e palavra pass.

1 – Para prevenir acessos não autorizados de utilizadores.

2 – Para apresentar uma mensagem de boas vindas personalizada.

3 – Para registar o tempo de utilização dos utilizadores.

4 –Para instalar software.

Sugestões de leitura:

Ao forçar o login num equipamento, é possível controlar quem tem acesso ao equipamento, controlar as permissões e direitos de um utilizador e controlar os recursos disponíveis.

Link de leitura sugerido:

https://docs.microsoft.com/pt-br/windows/security/threat-protection/security-policy-settings/user-rights-assignment

Compromisso de Aplicação

Pergunta: O que podes fazer para evitar a exploração de vulnerabilidades de uma aplicação instalada no teu computador?

1 – Manter instaladas as aplicações estritamente necessárias.

2 – Efetuar as atualizações de segurança lançadas pelo fabricante.

3 – Não instalar ou utilizar software adulterado.

4 – Todas as opções anteriores.

Sugestões de leitura:

Uma vulnerabilidade de software é normalmente uma deficiência ou falha de segurança num sistema operativo ou aplicações. Essas falhas podem ser exploradas para realizar ataques e conceder o controle do computador a um invasor ou colocar o software a realizar tarefas para que não foi projetado.

Apesar das atualizações de software parecerem um incômodo, são uma medida preventiva de segurança muito importante, adicionando de novos recursos, removendo recursos desatualizados, atualizando drivers, e aplicando correções para bugs entre outros.

Como medida adicional devem-se manter instaladas apenas as aplicações estritamente necessárias como forma de reduzir os riscos.

A utilização de software adulterado, representa um problema porque na maioria dos casos viola os direitos de autor, mas também por muitas vezes efetuar ações ocultas não relacionadas com a função para que foi projetado.

Link de leitura sugerido:

https://www.cncs.gov.pt/sistemas-atualizados/

https://br.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html

https://www.kaspersky.com.br/resource-center/preemptive-safety/antivirus-updates

Arrombamento

Pergunta: Qual dos seguintes pode prevenir o roubo de um computador?

1 – Utilizar um software antivírus.

2 – Ser monitorizado por uma camara web.

3 – Ter spyware.

4 – Estar ligado a um cabo de segurança.

Sugestões de leitura:

Com o computador/portátil amarrado a uma mesa ou superfície sólida e fixa com um cabo de segurança será mais difícil de roubar, afastando criminosos que procuram facilidade. Para além disso, considera etiquetá-lo.

Pergunta: Qual das seguintes afirmações define melhor porque se deve bloquear o computador quando se sai da secretária.

1 – Para prevenir o mau funcionamento do computador.

2 – Para poupar energia.

3 – Para evitar o acesso não autorizado aos dados.

4 – Para evitar a alteração dos dados.

Link de leitura sugerido:

https://www.cncs.gov.pt/content/files/3_en.pdf

https://www.cncs.gov.pt/content/files/brochura_2.pdf

Tentativa de Intrusão

Exploração de Vulnerabilidade

Pergunta: As atualizações do sistema operativo e do software devem estar configuradas para instalação automática porque:

1 – Adicionam novas funcionalidades.

2 – Incluem atualizações de segurança importantes e correções de bugs, permitindo que o software e dispositivos funcionem melhor e com mais segurança.

3 – Utilizam os recursos do sistema disponíveis.

4 – Todas as opções anteriores.

Sugestões de leitura:

Embora possa ser muito frustrante instalar as atualizações de software devido ao tempo que consome e pelas possíveis alterações no modo de funcionamento, as atualizações de software e sistema não contêm apenas novos recursos. Elas também incluem atualizações de segurança importantes e correções de bugs, permitindo que o software e dispositivos funcionem melhor e com mais segurança.

Link de leitura sugerido:

https://www.cncs.gov.pt/sistemas-atualizados/

Tentativa de Login

Pergunta: Qual das Palavras Passe seria considerada mais segura? Escolha a melhor resposta.

1 – Password123

2 – 654321

3 – joho0122

4 – Fa@t2H@7

Sugestões de leitura:

Uma Palavra Passe forte é composta pelo menos por oito caracteres e deve ser composta por uma combinação de letras maiúsculas e minúsculas, números e símbolos (@, #, $,%, etc.).
Se tens alguma dificuldade em lembrar as palavras-passe, um bom truque será usar a primeira letra das palavras que constituem uma frase ou por exemplo a letra de uma música.

Link de leitura sugerido:

https://www.cncs.gov.pt/content/files/password.pdf

https://www.cncs.gov.pt/content/files/enisa_posters_strong_password_tt.pdf

https://support.microsoft.com/pt-pt/windows/criar-e-utilizar-palavras-passe-seguras-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
https://blog.eset.pt/2012/03/como-criar-uma-palavra-passe-segura-e-da-qual-nao-se-esqueca/

Pergunta: Qual das Palavras Passe seria considerada menos segura? Escolhe a melhor resposta.

1 – Password#1

2 – 123456

3 – joho0122

4 – Todas as opções anteriores.

Sugestões de leitura:

Uma Palavra Passe forte é composta pelo menos por oito caracteres e deve ser composta por uma combinação de letras maiúsculas e minúsculas, números e símbolos (@, #, $,%, etc.).
Se tens alguma dificuldade em lembrar as palavras-passe, um bom truque será usar a primeira letra das palavras que constituem uma frase ou por exemplo a letra de uma música.

Link de leitura sugerido:

https://www.cncs.gov.pt/content/files/password.pdf

https://www.cncs.gov.pt/content/files/enisa_posters_strong_password_tt.pdf

https://support.microsoft.com/pt-pt/windows/criar-e-utilizar-palavras-passe-seguras-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
https://blog.eset.pt/2012/03/como-criar-uma-palavra-passe-segura-e-da-qual-nao-se-esqueca/

Pergunta: Qual seria o melhor método para guardar uma palavra pass?

1 – Guardar a palavra pass numa folha de excel.

2 – Guardar a palavra pass num post-it.

3 – Utilizar um gestor de passwords seguro.

4 – Todas as opções anteriores.

Sugestões de leitura:

A utilização de um gestor de passwords pode ser uma solução para guardar de forma segura um conjunto de passwords, no entanto, esta solução sempre que possível deve ser evitada devendo sempre que possível serem memorizadas.

Link de leitura sugerido:

https://www.cncs.gov.pt/content/files/password.pdf

https://www.cncs.gov.pt/content/files/enisa_posters_strong_password_tt.pdf

Pergunta: O que é a autenticação mutifator?

1 – Utilizar algo mais que a senha para entrar numa conta (ex: mensagem com um PIN).

2 – Método que permite o acesso a uma conta sem senha.

3 – Método de autenticação onde basta que um dos dados fornecidos esteja correto para permitir o acesso.

4 – Método de autenticação que não permite a utilização de dados biométricos como a impressão digital, a face, a voz ou reconhecimento da iris.

Sugestões de leitura:

Com a verificação em duas etapas ou autenticação mutifator, é uma camada extra de segurança para o caso de a senha ser roubada. Com a verificação em duas etapas ativa, o login

na conta é feito com algo que se sabe (como sua senha), e algo que se tem (como o telemóvel).

Link de leitura sugerido:

https://www.microsoft.com/pt-pt/security/business/identity-access-management/mfa-multi-factor-authentication
https://www.cncs.gov.pt/autenticacao-de-2-fatores/

Nova assinatura de ataque

Pergunta: Qual das afirmações indica porque é importante utilizar e atualizar o antivírus regulamente:

1 - Para identificar vírus antigos.

2 – Para proteger o sistema de todos os vírus conhecidos.

3 – Para prevenir a difusão de programas/apps maliciosas na internet.

4 – Para não receber mensagens não solicitadas no computador.

Sugestões de leitura:

Tendo em vista as pragas virtuais cada vez mais sofisticadas, a utilização de uma solução de segurança, como um bom antivírus, é essencial para garantir algum nível de proteção.

Link de leitura sugerido:

https://support.microsoft.com/pt-pt/windows/proteger-o-meu-pc-contra-v%C3%ADrus-b2025ed1-02d5-1e87-ba5f-71999008e026
https://blog.avast.com/pt-br/por-que-voce-deve-usar-um-antivirus

Pergunta: Todos os dias surgem centenas de novas assinaturas de ataque, que podem comprometer a segurança dos utilizadores online.

Que medidas podes adotar para uma proteção mais eficiente?

1 – Manter o antivírus ativo e atualizado.

2 – Instalar as atualizações do sistema operativo e atualizar ou remover todo o software desatualizado.

3 – Manter-me atento online à informação que recebo e ao funcionamento do meu equipamento.

4 –Todas as opções anteriores.

Sugestões de leitura:

Todos os dias surgem centenas de novas assinaturas de ataque, sendo a única forma de proteção a utilização de um antivírus atualizado e a funcionar para garantir algum nível de proteção contra o software malicioso.

Link de leitura sugerido:

https://support.microsoft.com/pt-pt/windows/proteger-o-meu-pc-contra-v%C3%ADrus-b2025ed1-02d5-1e87-ba5f-71999008e026
https://blog.avast.com/pt-br/por-que-voce-deve-usar-um-antivirus

Segurança da Informação

Acesso não autorizado

Pergunta: Obter acesso não autorizado a um sistema é conhecido como?

1 – Spamming.

2 – Hacking.

3 – Login.

4 – Cracking.

Sugestões de leitura:

Um hacker é um indivíduo que pretende obter acesso não autorizado a um sistema de computador.

O acesso não autorizado ocorre quando uma pessoa obtém acesso lógico ou físico sem permissão a uma rede, sistema, aplicativo, dados ou outro recurso (ex: site, programa, servidor, serviço).

Os utilizadores podem aumentar a sua segurança utilizando palavras pass fortes, instalando as atualizações dos sistemas operativos e aplicações sempre que são disponibilizadas, ter instalado antivírus e firewall, ser cauteloso quando ligado à internet, limitar o acesso aos equipamentos, entre outros.

Link de leitura sugerido:

https://www.cert.govt.nz/individuals/common-threats/unauthorised-access/

https://paginas.fe.up.pt/~als/mis10e/ch8/chpt8-1bullettext.htm

https://csrc.nist.gov/glossary/term/unauthorized_access

Modificação não autorizada

Pergunta: Qual dos seguintes não é considerado "alteração de dados sem permissão"?

1 – Alterar o montante de dinheiro numa conta bancária.

2 – Acesso a material de computador sem permissão.

3 – Escrever um vírus para destruir dados.

4 – Nenhuma das opções anteriores.

Sugestões de leitura:

A proteção contra modificação não autorizada, pretende garantir que as informações permaneceram inalteradas desde o ponto em que foram produzidas por uma fonte, durante a transmissão, armazenamento e eventual recebimento pelo destinatário.

Link de leitura sugerido:

https://www.cncs.gov.pt/recursos/glossario/

https://study.com/academy/lesson/information-security-basic-principles.html

Perda de dados

Pergunta: Qual das opções seguintes não oferece proteção contra o uso indevido ou modificação de dados num sistema?

1 – Criação de backups regulares.

2 – Dar a cada utilizador um nome de usuário e uma senha.

3 – Permitir que os utilizadores tenham acesso completo ao sistema e confiar que eles acedem apenas aos seus dados.

4 – Nenhuma das opções anteriores.

Sugestões de leitura:

A perda ou o roubo de dados podem ter consequências graves. Algumas das informações pessoais armazenadas podem ser de difícil recuperação, ou abrir portas para que criminosos roubem a identidade digital ou dinheiro.

A proteção mais eficiente contra este tipo de ataques passa por utilizar um software antimalware para evitar infeções. É também importante, fazer backups frequentes das informações armazenadas, pois assim mesmo que sejam infetados por um software malicioso, ocorra uma falha num disco rígido ou outro componente dificulte o acesso à informações a sua recuperação será possível recorrendo ao backup dos dados.

Link de leitura sugerido:

https://www.kaspersky.com.br/resource-center/threats/data-theft

Fraude

Utilização indevida ou não autorizada de recursos

Pergunta: A mineração de criptomoeda de forma ilegal pode infetar os equipamentos por:

1 – Visita de websites infetados.

2 – Pela utilização de software pirateado.

3 – Infeção com malware.

3 – Todas as opções anteriores.

Sugestões de leitura:

A mineração de criptomoedas ilegal ou, Criptojacking é um esquema utilizado para explorar os dispositivos das pessoas (computadores, smartphones, tablets ou mesmo servidores), sem o seu consentimento ou conhecimento, com o objetivo de minerar, secretamente, criptomoeda às custas da vítima.

Os hackers utilizam o criptojacking para roubar recursos computacionais dos dispositivos das suas vítimas, abrandando os restantes processos, aumenta a fatura de eletricidade e encurta a vida útil dos dispositivos. Consoante o quão subtil é o ataque, podem ser detetados alguns sinais de alerta, como o PC ou Mac ficar mais lento ou utilizar a ventoinha de refrigeração mais vezes que o normal.

Link de leitura sugerido:

https://pt.malwarebytes.com/cryptojacking/

https://www.hornetsecurity.com/en/knowledge-base/crypto-mining/

Pergunta: Qual das afirmações seguintes é verdade em relação a sistemas infetados com software de mineração ilícito:

1 – Só afeta sistemas operativos Windows.

2 – Utiliza muito processador, tornado lento ou impedindo a utilização do equipamento pelo utilizador.

3 – Não é capaz de contornar programas antivírus.

4 -Todas as opções anteriores.

Sugestões de leitura:

A mineração de criptomoedas ilegal ou, Criptojacking é um esquema utilizado para explorar os dispositivos das pessoas (computadores, smartphones, tablets ou mesmo servidores), sem o seu consentimento ou conhecimento, com o objetivo de minerar, secretamente, criptomoeda às custas da vítima.

Os hackers utilizam o criptojacking para roubar recursos computacionais dos dispositivos das suas vítimas, abrandando os restantes processos, aumenta a fatura de eletricidade e encurta a vida útil dos dispositivos. Consoante o quão subtil é o ataque, podem ser detetados alguns sinais de alerta, como o PC ou Mac ficar mais lento ou utilizar a ventoinha de refrigeração mais vezes que o normal.

Link de leitura sugerido:

https://pt.malwarebytes.com/cryptojacking/

https://www.hornetsecurity.com/en/knowledge-base/crypto-mining/

Direitos de autor

Pergunta: Se uma obra é de domínio publico, significa que:

1 – Está disponível numa biblioteca publica.

2 – É possível obter a informação online.

3 – Podes copiar sem ter de pedir permissão.

4 – Nenhuma das opções anteriores.

Sugestões de leitura:

O direito de autor é a designação do direito que protege as criações literárias e artísticas, conferindo ao autor um direito de exploração económica exclusivo, com o poder de autorizar terceiros de usar a sua criação/obra, e ainda direitos pessoais ou morais que asseguram o respeito pelo contributo pessoal do autor. A proteção conferida pelo direito de autor incide sobre a expressão ou manifestação (forma) das criações/obras, e não sobre as ideias que estão na sua base.

Link de leitura sugerido:

https://www.internetsegura.pt/DireitosAutor

https://euipo.europa.eu/ohimportal/pt/web/observatory/faqs-on-copyright-pt#1

Pergunta: O que é copyright?

1 – Uma forma de proteger o trabalho do criador.

2 – Um título.

3 – É crime, e a pena pode ser de reclusão e/ou multa.

4 – Nenhuma das opções anteriores.

Sugestões de leitura:

O direito de autor é a designação do direito que protege as criações literárias e artísticas, conferindo ao autor um direito de exploração económica exclusivo, com o poder de autorizar terceiros de usar a sua criação/obra, e ainda direitos pessoais ou morais que asseguram o respeito pelo contributo pessoal do autor. A proteção conferida pelo direito de autor incide sobre a expressão ou manifestação (forma) das criações/obras, e não sobre as ideias que estão na sua base.

Link de leitura sugerido:

https://copyrightalliance.org/faqs/what-is-copyright/

https://www.copyright.gov/help/faq/faq-definitions.html

https://www.internetsegura.pt/DireitosAutor

https://euipo.europa.eu/ohimportal/pt/web/observatory/faqs-on-copyright-pt#1

Pergunta: Quando compras um software o que estás a comprar?

1 – O direito de usar o software sob os termos da licença.

2 – O software.

3 – O copyright.

4 – Todas as opções anteriores.

Sugestões de leitura:

Uma licença de software é um documento formal sobre um software, e a sua função principal é estabelecer os termos e garantias para quem desenvolveu o software a respeito.

Link de leitura sugerido:

https://triplait.com/licenciamento-de-software-o-guia/

Pergunta: O que é pirataria de software?

1 - Roubo e violência no mar.

2 - Transmissão FM ilegal.

3 - Cópia ilegal de material protegido por copyright.

4 – Todas as opções anteriores.

Sugestões de leitura:

A pirataria de software e a cópia ilegal, é uma cópia idêntica de um sistema de computador (programas, sistemas operacionais, etc) ou de um CD de música convencional. Só que essa mesma cópia idêntica é distribuída ilegalmente (sem um número de registo e sem a licença dos detentores dos direitos autorais).

Link de leitura sugerido:

https://www.asae.gov.pt/fiscalizacao-economica/informacoes-sobre-atividades-economicas/pirataria-informatica.aspx

Pergunta: Para não cometeres plágio, deves...

1 – Ao fazer citações, referir sempre os seus autores, colocando o texto entre aspas.

2 – Fazer referência aos autores dos documentos que utilizas, na bibliografia.

3 – Usa as tuas próprias palavras.

4 – Todas as opções anteriores.

Sugestões de leitura:

O plágio acontece quando alguém copia um conteúdo produzido por outra pessoa sem apresentar a fonte original, podendo acontecer com vários tipos de conteúdos, como trabalhos acadêmicos, livros, músicas e imagens.

Link de leitura sugerido:

https://www.infopedia.pt/dicionarios/lingua-portuguesa/pl%C3%A1gio

https://copyleaks.com/pt/plagiarism-checker/what-is-plagiarism

Pergunta: Se encontrares um site com conteúdos que apelam ao ódio e à violência, deves...

1 – Fazer nova pesquisa ignorando o site encontrado.

2 – Denunciar o site por conteúdos ilegais.

3 – Partilhar com todos os teus contactos o link do site e manifestar a tua indignação.

4 – Todas as opções anteriores.

Sugestões de leitura:

O discurso de incentivo ao ódio é um ataque contra pessoas com base nas suas caraterísticas: raça, etnia, nacionalidade, deficiência, afiliação religiosa, casta, orientação sexual, sexo, identidade de género e doença grave.

Link de leitura sugerido:

https://pt-pt.facebook.com/communitystandards/hate_speech

http://www.odionao.com.pt/

https://www.sosracismo.pt/geral/contra-o-incitamento-ao-odio-e-a-violencia

Utilização ilegítima de nome de terceiros (roubo de identidade)

Pergunta: O que é roubo de identidade?

1 – Quando alguém usa informações de identificação pessoais de outras pessoas sem permissão, cometendo fraudes e outros crimes.

2 – Quando um utilizador é reencaminhado para uma cópia fraudulenta de um website legítimo.

3 – Ocorre quando não são adotadas medidas de segurança suficientes para efetuar pesquisas na Internet.

4 – Ocorre quando um utilizador utiliza o nickname de outro para se registar num chat.

Sugestões de leitura:

Os ladrões de identidade geralmente procuram obter informação pessoal como senhas, números de identidade, números de cartão de crédito ou CPF.

Os casos de roubo de identidade devem ser imediatamente denunciados às autoridades, bem como outro tipo de abusos ou violência. A Polícia Judiciária tem competência para investigar crimes relacionados com utilizações abusivas de redes informáticas.

Link de leitura sugerido:

https://www.eset.com/br/furto-identidade/

https://www.avg.com/pt/signal/identity-theft

https://apav.pt/publiproj/index.php/52-projeto-proteus-apoio-a-vitimas-de-furto-de-identidade-e-fraude-de-identidade

Pergunta: Se suspeitar que foi vítima de roubo de identidade, o se deve fazer?

1 – Deixa de seguir as publicações, ignorar a situação faz com que o problema deixe de acontecer.

2 – Cancelar o cartão de crédito é suficiente.

3 – Entra em contato com a instituição bancária, reporta ás autoridades policiais e manter registros meticulosos e cópias de todas as ações tomadas.

4 - Nenhuma das opções anteriores.

Sugestões de leitura:

Os ladrões de identidade geralmente procuram obter informação pessoal como senhas, números de identidade, números de cartão de crédito ou CPF.

Os casos de roubo de identidade devem ser imediatamente denunciados às autoridades, bem como outro tipo de abusos ou violência. A Polícia Judiciária tem competência para investigar crimes relacionados com utilizações abusivas de redes informáticas.
Link de leitura sugerido:

https://www.eset.com/br/furto-identidade/

https://www.avg.com/pt/signal/identity-theft

https://apav.pt/publiproj/index.php/52-projeto-proteus-apoio-a-vitimas-de-furto-de-identidade-e-fraude-de-identidade

Pergunta: A cópia de fotos e a sua utilização abusiva, descontextualizando-as ou usando-as sem autorização em perfis falsos.

O que podes fazer evitar que as tuas fotos sejam usadas, abusivamente?

1 – Inclusão de referências aos direitos de autor das imagens.

2 – Recorrer à pesquisa reversa de imagens disponibilizada pelo Google.

3 – Introdução de marcas de água em imagens.

4 – Todas as opções anteriores.

Sugestões de leitura:

No contexto de relacionamentos online, as pessoas tendem a partilhar mensagens, vídeos ou imagens.

A disponibilização de quaisquer fotografias não implica a permissão automática da sua utilização por toda e qualquer pessoa podendo estar sujeita a direitos de proteção da imagem dos retratados, e à proteção do trabalho fotográfico em sede de direitos de autor.

Link de leitura sugerido:

https://www.apav.pt/cibercrime/

https://ipf.pt/site/uso-fotos-livremente-acessiveis-no-facebook-pode-crime/

https://lms.nau.edu.pt

Phishing

Pergunta: Um exemplo de ataque de Phishing é:

1 – Enviar a alguém uma mensagem com um link malicioso disfarçado de mensagem a informar que ganhou um prémio.

2 – Enviar um email com um link malicioso que se parece uma mensagem de alguém que conhece.

3 – Criar um website idêntico a um real (fidedigno) para levar os utilizadores a introduzirem os seus dados de login.

4 – Todas as opções anteriores

Sugestão de leitura:

Phishing é uma técnica de ciber crime que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.

A sal distribuição pode ser feita por e-mail, redes sociais, SMS ou de outras formas, seguindo sempre os mesmos princípios básicos. O burlão envia um texto direcionado, com o objetivo de convencer a vítima a clicar num link, transferir um anexo, enviar informações ou efetuar um pagamento real.

Link de leitura sugerido:

https://www.avast.com/pt-br/c-phishing

https://pt.malwarebytes.com/phishing/

https://www.avg.com/pt/signal/what-is-phishing

Pergunta: Phishing é:

1 - Um jogo online que incentiva os utilizadores a cometerem ações perigosas contra si mesmos.

2 - Uma estratégia que pretende enriquecer rapidamente os utilizadores.

3 - Um método criminoso pelo qual se capturam credenciais de acesso a contas, para depois aceder ilegalmente às mesmas e, com isso, obter vantagens.

4 – Nenhuma das opções anteriores.

Sugestão de leitura:

Phishing é uma técnica de ciber crime que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.

A sal distribuição pode ser feita por e-mail, redes sociais, SMS ou de outras formas, seguindo sempre os mesmos princípios básicos. O burlão envia um texto direcionado, com o objetivo de convencer a vítima a clicar num link, transferir um anexo, enviar informações ou efetuar um pagamento real.

Link de leitura sugerido:

https://www.avast.com/pt-br/c-phishing

https://pt.malwarebytes.com/phishing/

https://www.avg.com/pt/signal/what-is-phishing

Pergunta: Um e-mail suspeito deve ser excluído quando? Escolhe a melhor resposta.

1 – Endereço é longo e confuso e o nome do remetente é vago.

2 - O assunto do e-mail é apelativo (grande oferta ou desconto) ou alarmista.

3 – O e-mail pede que se clique em textos com hiperlinks.

4 – Todas as opções anteriores.

Sugestão de leitura:

Phishing é uma técnica de ciber crime que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.

A sal distribuição pode ser feita por e-mail, redes sociais, SMS ou de outras formas, seguindo sempre os mesmos princípios básicos. O burlão envia um texto direcionado, com o objetivo de convencer a vítima a clicar num link, transferir um anexo, enviar informações ou efetuar um pagamento real.

Link de leitura sugerido:

https://www.avast.com/pt-br/c-phishing

https://pt.malwarebytes.com/phishing/

https://www.avg.com/pt/signal/what-is-phishing

Pergunta: Um e-mail suspeito deve ser excluído quando? Escolhe a melhor resposta.

1 – Palavras com erros ortográficos e/ou frases com gramática incorreta.

2 – Tenta assustar-te, para incentivar que cliques em alguma coisa.

3- A oferta, parece boa demais para ser verdade.

4 – Todas as opções anteriores.

Sugestão de leitura:

Phishing é uma técnica de ciber crime que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.

A sal distribuição pode ser feita por e-mail, redes sociais, SMS ou de outras formas, seguindo sempre os mesmos princípios básicos. O burlão envia um texto direcionado, com o objetivo de convencer a vítima a clicar num link, transferir um anexo, enviar informações ou efetuar um pagamento real.

Link de leitura sugerido:

https://www.avast.com/pt-br/c-phishing

https://pt.malwarebytes.com/phishing/

https://www.avg.com/pt/signal/what-is-phishing

Conteúdo Abusivo

SPAM

Pergunta: Qual é o nome dado ao software que monitoriza um sistema em busca de e-mails indesejados?

1 – Filtro de SPAM.

2 – Detetor de spyware.

3 – Firewall.

4 – Bloqueador de phishing.

Sugestões de leitura:

O termo “spam” é utilizado para identificar mensagens invasivas não solicitadas enviadas em massa pela internet, recorrendo a sistemas de mensagens eletrônicas.

Link de leitura sugerido:

https://www.avast.com/pt-br/c-spam

https://www.cncs.gov.pt/recursos/boas-praticas/

https://www.cncs.gov.pt/content/files/alerta_-_email.pdf

https://www.apav.pt/cibercrime/

Pergunta: Qual dos seguintes serviços é utilizado para propagar SPAM?

1 – Chat

2 – WWW

3 – Email

4 – Nenhum dos anteriores

Sugestões de leitura:

O termo “spam” é utilizado para identificar mensagens invasivas não solicitadas enviadas em massa pela internet, recorrendo a sistemas de mensagens eletrônicas.

Link de leitura sugerido:

https://www.avast.com/pt-br/c-spam

https://www.cncs.gov.pt/recursos/boas-praticas/

https://www.cncs.gov.pt/content/files/alerta_-_email.pdf

https://www.apav.pt/cibercrime/

Discurso Nocivo

Pergunta: Qual das seguintes melhor define o que é cyberbulling?

1 – Cyberbulling acontece quando alguém está a ser repetidamente atacado fisicamente na escola ou noutro lugar.

2 – Cyberbulling acontece quando se recebe uma mensagem maldosa nas redes sociais.

3 – Cyberbulling refere-se a qualquer ato de bullying que acontece online de forma repetida.

4 – Cyberbooling acontece quando se cria amigos online sem os conhecer em pessoa.

Sugestões de leitura:

Atualmente a comunicação privilegia os meios eletrónicos e faz-se através das redes sociais, das SMS, do WhatsApp, entre outros.

O Cyberbullying refere-se a qualquer comportamento de bullying que ocorre "virtualmente" usando dispositivos e plataformas, podendo ocorrer a qualquer hora desde que estejam ligados à internet.

Link de leitura sugerido:

https://www.sembullyingsemviolencia.edu.gov.pt/

https://www.portoeditora.pt/paisealunos/pais-and-alunos/noticia/ver/?id=28305&langid=1

Pergunta: Se tivesses conhecimento de alguma situação de cyberbulling o que devias fazer?

1 – Não fazer nada.

2 - Pedir ajuda, e fazer o teu melhor para ajudar e proteger a pessoa que está a ser atacada.

3 – Enfrentar o atacante, falando com ele em frente de todos.

4 – Nenhuma das opções anteriores.

Sugestões de leitura:

Atualmente a comunicação privilegia os meios eletrónicos e faz-se através das redes sociais, das SMS, do WhatsApp, entre outros.

O *Cyberbullying* refere-se a qualquer comportamento de *bullying* que ocorre "virtualmente" usando dispositivos e plataformas, podendo ocorrer a qualquer hora desde que estejam ligados à internet.

Link de leitura sugerido:

https://www.sembullyingsemviolencia.edu.gov.pt/

https://www.portoeditora.pt/paisealunos/pais-and-alunos/noticia/ver/?id=28305&langid=1

Pergunta: Vês uma pessoa a ser 'envergonhada' no Facebook.

Tu não conheces essa pessoa e há muitas pessoas a participar com comentários ofensivos.

O que deves fazer?

1 – Partilhar com os teus amigos porque é divertido.

2 – Denunciar a situação e fazer comentários positivos.

3 – Podes fazer Like, mas não deixar comentários negativos.

4 – Nenhuma das opções anteriores.

Sugestões de leitura:

Atualmente a comunicação privilegia os meios eletrónicos e faz-se através das redes sociais, das SMS, do WhatsApp, entre outros.

O *Cyberbullying* refere-se a qualquer comportamento de *bullying* que ocorre "virtualmente" usando dispositivos e plataformas, podendo ocorrer a qualquer hora desde que estejam ligados à internet.

Link de leitura sugerido:

https://www.sembullyingsemviolencia.edu.gov.pt/

https://www.portoeditora.pt/paisealunos/pais-and-alunos/noticia/ver/?id=28305&langid=1

Exploração sexual de menores, racismo e apologia da violência

Pergunta: Sexting é um termo utilizado para se referir à divulgação de conteúdos eróticos e sensuais através online.

Porque não deves partilhar qualquer conteúdo que possa ser considerado erótico ou sexual online:

1 – Existe o risco de essas fotos se tornaram públicas.
2 – Existe o risco de assédio moral, abuso emocional, pornografia de vingança, assédio.
3 – Existe o risco de extorsão.
4 – Todas as opções anteriores.

Sugestões de leitura:

Sexting é a prática de enviar conteúdos íntimos através de dispositivos ou através das redes sociais, em forma de texto, de fotos ou de vídeo.

Link de leitura sugerido:

https://www.seguranet.pt/pt/sexting-0

https://apav.pt/publiproj/images/yootheme/PDF/Hate_No_More_Procedures_Handbook_PT.pdf

https://infovitimas.pt/pt/001_home/001_infovictms.html

https://apav.pt/care/index.php/informacao-para-adult-s/12-perguntas-e-respostas-sobre-violencia-sexual-contra-criancas-e-jovens

Pergunta: Qual das seguintes opções explica melhor o que é o sexting?

1 - Vídeos publicados em sites para adultos.

2 - Vídeos publicados nas redes sociais.

3 - Termo usado para descrever o envio de mensagens, fotografias e vídeos sexualmente explícitos ou agressivos, normalmente por telemóvel.

4 – Todas as opções anteriores.

Sugestões de leitura:

Sexting é a prática de enviar conteúdos íntimos através de dispositivos ou através das redes sociais, em forma de texto, de fotos ou de vídeo.

Link de leitura sugerido:

https://www.seguranet.pt/pt/sexting-0

https://apav.pt/publiproj/images/yootheme/PDF/Hate_No_More_Procedures_Handbook_PT.pdf

https://infovitimas.pt/pt/001_home/001_infovictms.html

https://apav.pt/care/index.php/informacao-para-adult-s/12-perguntas-e-respostas-sobre-violencia-sexual-contra-criancas-e-jovens

Vulnerabilidade

Criptografia fraca

Pergunta: Das seguintes qual descreve a melhor forma de enviar informação confidencial numa rede não segura.

1 – Num ficheiro comprimido.

2 – Num ficheiro encriptado.

3 – Num email normal.

4 – Num anexo.

Sugestões de leitura:

Criptografia é a prática de codificar e decodificar dados. Quando os dados são encriptados, é aplicado um algoritmo para codificá-los de modo que eles não tenham o formato original e, portanto, não possam ser lidos. Estes são designados por ficheiros encriptados, e o seu conteúdo só pode ser obtido revertendo o processo.

Link de leitura sugerido:

https://www.kaspersky.com.br/resource-center/definitions/encryption

Pergunta: Se queres enviar uma mensagem encriptada com PGP, primeiro terás de saber?

1 – Chave privada do destinatário.

2 – Chave publica do destinatário.

3 –A tua chave publica.

4 – HASH da mensagem a enviar.

Sugestões de leitura:

O PGP é um sistema de criptografia usado para enviar e-mails criptografados, mas também permite encriptar qualquer informação pessoal ou privada (seja um e-mail, um ficheiro ou todo o disco rígido) tornando muito difícil espiar ou intercetar o conteúdo.
Conhecendo a chave publica de um destinatário é possível encriptar uma mensagem que só poderá ser lida pelo detentor da chave privada associada á chave publica utilizada.

Link de leitura sugerido:

https://www.kaspersky.com/blog/pgp-reliable-privacy-security-and-authentication-for-everyone/3031/

Amplificador DDoS

Pergunta: Qual das opções seguintes melhor define o que é um ataque de DDOS?

1 – Um ataque de negação de serviço distribuída (DDOS) destina-se a interromper um serviço impedindo a sua utilização pelos utilizadores, recorrendo a uma rede de BotNet.

2 – Recorre a uma rede zumbi (BotNet), para distribuir código malicioso por computadores ligados à internet.

3 – Este tipo de ataque é fácil de detetar e bloquear.

4 – Todas as opções anteriores.

Sugestões de leitura:

Os ataques de negação de serviço distribuído (DDoS), têm como objetivo limitar a capacidade das redes, servidores, e a disponibilidade de serviços em rede (ex: páginas de internet).

Funciona com base no envio de múltiplas solicitações para o recurso, para que exceda a sua capacidade de resposta e impedindo assim a resposta a solicitações reais.

Link de leitura sugerido:

https://www.cloudflare.com/pt-br/learning/ddos/ddos-attack-tools/how-to-ddos/

https://www.avg.com/pt/signal/what-is-ddos-attack

https://www.kaspersky.com.br/resource-center/threats/ddos-attacks

Pergunta: Dos seguintes, qual não é um sintoma de ataque de DDOS ?

1 – Resposta às solicitações de informação muito mais lenta do que o normal.

2 – Algumas ou todas as solicitações dos utilizadores totalmente ignoradas.

3 – Acesso não autorizado à informação.

4 – Todas as opções anteriores.

Sugestões de leitura:

Os ataques de negação de serviço distribuído (DDoS), têm como objetivo limitar a capacidade das redes, servidores, e a disponibilidade de serviços em rede (ex: páginas de internet).

Funciona com base no envio de múltiplas solicitações para o recurso, para que exceda a sua capacidade de resposta e impedindo assim a resposta a solicitações reais.

Link de leitura sugerido:

https://www.cloudflare.com/pt-br/learning/ddos/ddos-attack-tools/how-to-ddos/

https://www.avg.com/pt/signal/what-is-ddos-attack

https://www.kaspersky.com.br/resource-center/threats/ddos-attacks

Serviços acessíveis potencialmente indesejados

Pergunta: Quais dos serviços seguintes, devem ser desativados se estiverem acessíveis no teu computador:

1 – Servidor NFS, servidor DNS.

2 – Servidor web, Servidor FTP.

3 – Telnet, RDP ou VNC.

4 – Todas as opções anteriores.

Sugestões de leitura:

Serviços como o Telnet, RDP ou VNC ao estarem acessíveis num equipamento pessoal devem ser removidos pois podem comprometer a privacidade ou enfraquecer a segurança do computador.

Revelação de informação

Pergunta: Qual das seguintes seria uma atividade insegura online:

1 – Utilizar um nickname que não permite a tua identificação online.

2 – Encontares-te com alguém que conheceste online com os teus pais.

3 – Manter o teu perfil de rede social privado.

4 – Dar a tua morada de casa a algum que conheceste online numa sala de conversação.

Sugestões de leitura:

A partilha de informação pessoais, imagens, eventos, a criação de relações de "amizade", e a partilha de comportamentos diários online representa um grande risco para os utilizadores.

Os utilizadores, devem minimizar a informação que partilham pensando muito bem antes de o fazer, pois uma simples fotografia pode dar informações a terceiros que sem nos apercebemos.

Link de leitura sugerido:

https://www.youtube.com/watch?v=og4uRmN4NAM

https://ensina.rtp.pt/artigo/seguranet-cuidado-com-a-partilha-de-informacao-pessoal/

https://blog.eset.pt/2018/07/redes-sociais-o-problema-e-partilhar-em-demasia/

https://pplware.sapo.pt/redes_sociais/partilha-redes-sociais-cuidado/

Pergunta: Para manteres as tuas informações seguras não as deves partilhar online.

Qual das opções seguintes representa informação que podes partilhar online sem risco:

1 – A tua morada ou da tua escola.

2 – Contacto telefónico.

3 – Fotos tuas.

4 – Nenhuma das opções anteriores.

Sugestões de leitura:

A partilha de informação pessoais, imagens, eventos, a criação de relações de "amizade", e a partilha de comportamentos diários online representa um grande risco para os utilizadores.

Os utilizadores, devem minimizar a informação que partilham pensando muito bem antes de o fazer, pois uma simples fotografia pode dar informações a terceiros que sem nos apercebemos.

Link de leitura sugerido:

https://www.youtube.com/watch?v=og4uRmN4NAM

https://ensina.rtp.pt/artigo/seguranet-cuidado-com-a-partilha-de-informacao-pessoal/

https://blog.eset.pt/2018/07/redes-sociais-o-problema-e-partilhar-em-demasia/

https://pplware.sapo.pt/redes_sociais/partilha-redes-sociais-cuidado/

Sistema vulnerável

Pergunta: Qual dos seguintes melhor descreve a função de uma FIREWALL:

1 – Proteger o computador caso ocorra um incendio.

2 – Para facilitar o download de programas /apps de um website.

3 – Para detetar e eliminar vírus do no computador.

4 – Para evitar acessos não autorizados com origem em ligações externas.

Sugestões de leitura:

As firewalls, podem ser programas de software ou dispositivos de hardware que têm como função filtrar e examinam as informações provenientes da ligação à Internet.

Representam a primeira linha de defesa porque podem impedir que programas maliciosos ou atacantes tenham acesso à rede e às informações.

Link de leitura sugerido:

https://nordvpn.com/pt-br/blog/o-que-e-firewall/

https://www.mcafee.com/pt-pt/antivirus/firewall.html

https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html

Pergunta: Qual das afirmações é verdadeira quando nos referimos a redes WIFI.

1 – Limitam o acesso aos utilizadores.

2 – Podem estar acessíveis a outros utilizadores.

3 – Não podem ser intersetadas por outros utilizadores.

4 – Podem limitar a visibilidade a outros utilizadores.

Sugestões de leitura:

As redes WIFI, geralmente são, o ponto de acesso mais fácil e com menos consequências para quem quer entrar indevidamente quando não existem os cuidados de segurança básicos.

Link de leitura sugerido:

https://www.deco.proteste.pt/tecnologia/antivirus/dicas/como-proteger-a-rede-domestica

https://blog.avast.com/pt-br/o-que-e-a-chave-de-seguranca-de-rede-e-como-utiliza-la

https://blog.eset.pt/2020/01/guia-sobre-como-configurar-o-seu-router-para-otimizar-a-seguranca-da-sua-rede-wi%E2%80%91fi/

Pergunta: Qual seria a melhor opção para proteger o acesso a uma rede WIFI?

1 – WEP

2 – WPA

3 – AES

4 – WPA2-PSK

Sugestões de leitura:

As redes WIFI, geralmente são, o ponto de acesso mais fácil e com menos consequências para quem quer entrar indevidamente quando não existem os cuidados de segurança básicos.

Algumas das medidas que devem ser adotadas são:

- Mude a password e o nome da rede *wi-fi* e do router.
- Utilizar o modo de segurança adequado (mais seguro).
- Crie redes *wi-fi* separada para visitantes.
- Oculte o nome de uma rede wi-fi (SSID).
- etc.

Link de leitura sugerido:

https://www.deco.proteste.pt/tecnologia/antivirus/dicas/como-proteger-a-rede-domestica

https://br.norton.com/internetsecurity-emerging-threats-what-to-do-about-krack-vulnerability.html

https://pplware.sapo.pt/microsoft/windows/10-dicas-para-proteger-a-sua-rede-wireless/

https://www.e-konomista.pt/como-proteger-a-rede-wi-fi/

Outro

Indeterminado/Sem tipo

Pergunta: As notícias falsas são um problema que tem de ser combatido.

Como podes contribuir para a sua eliminação online.

1 – Não promover o discurso de odio e as notícias falsas.

2 – Navegar apenas em websites fidedignos e com https.

3 – Utilizar uma VPN.

4 – Evitar conteúdos ilegais.

Sugestões de leitura:

As notícias falsas são um problema crescente e representam um perigo principalmente para aqueles que não desenvolvem sentido crítico.

O termo notícias falsas («*fake news*», em inglês) massificou-se e é muitas vezes usado como sinónimo de desinformação e de manipulação de informação.

Normalmente está associado a informação que circula na Internet, com o objetivo de enganar as pessoas em relação à realidade – seja para defender um ponto de vista, para acusar alguém, para ganhar dinheiro com *pageviews, likes* e publicidade, para vender produtos, para burlar consumidores ou, simplesmente, para impressionar os amigos.

Link de leitura sugerido:

https://www.nau.edu.pt/pt/curso/cidadao-ciberinformado/

https://www.cncs.gov.pt/content/files/campanha_contra_a_desinformao_2.pdf

https://www.cncs.gov.pt/recursos/noticias/cidadao-ciberinformado-testa-conhecimento-acerca-de-desinformacao/

https://combatefakenews.lusa.pt/o-projeto-combate-as-fake-news-contra-fake/

Pergunta: O que deves fazer para identificar uma notícia falsa? Escolhe a melhor resposta.

1 – Não partilhar lendo apenas o título.

2 – Uma imagem não vale por mil palavras, pois pode ser falsa.

3 – Confere a veracidade consultando fontes reconhecidas.

4 - Todas as opções anteriores.

Sugestões de leitura:

As notícias falsas são um problema crescente e representam um perigo principalmente para aqueles que não desenvolvem sentido crítico.

O termo notícias falsas («*fake news*», em inglês) massificou-se e é muitas vezes usado como sinónimo de desinformação e de manipulação de informação.

Normalmente está associado a informação que circula na Internet, com o objetivo de enganar as pessoas em relação à realidade – seja para defender um ponto de vista, para acusar alguém, para ganhar dinheiro com *pageviews, likes* e publicidade, para vender produtos, para burlar consumidores ou, simplesmente, para impressionar os amigos.

Link de leitura sugerido:

https://www.nau.edu.pt/pt/curso/cidadao-ciberinformado/

https://www.cncs.gov.pt/content/files/campanha_contra_a_desinformao_2.pdf

https://www.cncs.gov.pt/recursos/noticias/cidadao-ciberinformado-testa-conhecimento-acerca-de-desinformacao/

https://combatefakenews.lusa.pt/o-projeto-combate-as-fake-news-contra-fake/

Pergunta: Quando estás a navegar online, as páginas de internet (websites) podem recolher que informações sobre ti:

1 – Que programas utilizo.

2 – A minha localização aproximada online.

3 – As minhas preferências, como a língua em que vejo as páginas, em que clico e quanto tempo passo nas páginas.

4 – Todas as opções anteriores.

Sugestões de leitura:

As páginas de internet muitas vezes utilizam "*cookies*", as "*cookies*" são pequenos ficheiros que podem recolher informação sobre os utilizadores, como o endereço IP do computador, as preferências de visualização de determinada página.

Em alguns casos podem também guardar informação sobre as páginas que foram visitadas e durante quanto tempo lá se permaneceu.

Link de leitura sugerido:

https://www.allaboutcookies.org/

https://www.microsoft.com/info/cookies.mspx

B.3 EXEMPLO DE QUESTIONÁRIO DE AUTODIAGNÓSTICO GERADO

Pergunta **1**

Resposta guardada

Nota: 1,0

Qual das seguintes opções pode levar à disseminação de um programa malicioso?

1. Manter o antivírus atualizado.
2. Utilizar apenas software que foi verificado para a presença de vírus.
3. Utilizar um dispositivo USB de uma fonte desconhecida para trocar dados.
4. Abrir apenas anexos onde foi verificada a presença de vírus e de fontes conhecidas.

Limpar a minha escolha

Pergunta **2**

Resposta guardada

Nota: 1,0

A sabotagem de computadores:

1. acontece por ação deliberada de um utilizador.
2. pode envolver o uso de malware, como bots, worms, vírus e outros spywares.
3. pode passar por permitir o acesso indevido aos equipamentos ou eliminar informação.
4. Todas as opções anteriores.

Limpar a minha escolha

Pergunta **3**

Resposta guardada

Nota: 1,0

Pergunta **4**

Resposta guardada

Nota: 1,0

Como podes melhorar a tua segurança online?

1. Utilizar autenticação de duas etapas para aceder às tuas suas contas.
2. Configurar alertas, para que cada vez que se acede de um novo dispositivo a uma conta, sejas not
3. Utilizar palavras pass exclusivas para cada conta online e atualizá-las periodicamente.
4. Todas as opções anteriores.

Limpar a minha escolha

Pergunta **5**

Resposta guardada

Nota: 1,0

O que é a autenticação mutifator?

1. Utilizar algo mais que a senha para entrar numa conta (ex: mensagem com um PIN).
2. Método que permite o acesso a uma conta sem senha.
3. Método de autenticação onde basta que um dos dados fornecidos esteja correto para permitir o a
4. Método de autenticação que não permite a utilização de dados biométricos como a impressão dig reconhecimento da iris.

Limpar a minha escolha

Pergunta **6**

Resposta guardada

Nota: 1,0

Qual dos seguintes não é considerado "alteração de dados sem permissão"?

1. Alterar o montante de dinheiro numa conta bancária.
2. Acesso a material de computador sem permissão.
3. Escrever um vírus para destruir dados.
4. Nenhuma das opções anteriores.

Pergunta **7**

Resposta guardada

Nota: 1,0

O que é roubo de identidade?

1. Quando alguém usa informações de identificação pessoais de outras pessoas sem permissão, com crimes.
2. Quando um utilizador é reencaminhado para uma cópia fraudulenta de um website legítimo.
3. Ocorre quando não são adotadas medidas de segurança suficientes para efetuar pesquisas na Inte
4. Ocorre quando um utilizador utiliza o nickname de outro para se registar num chat.

Limpar a minha escolha

Pergunta **8**

Resposta guardada

Nota: 1,0

Sexting é um termo utilizado para se referir à divulgação de conteúdos eróticos e sensuais através o

Porque não deves partilhar qualquer conteúdo que possa ser considerado erótico ou sexual online:

1. Existe o risco de essas fotos se tornaram públicas.
2. Existe o risco de assédio moral, abuso emocional, pornografia de vingança, assédio.
3. Existe o risco de extorsão.
4. Todas as opções anteriores.

Limpar a minha escolha

Pergunta **9**

Resposta guardada

Nota: 1,0

Dos seguintes, qual não é um sintoma de ataque de DDOS ?

1. Resposta às solicitações de informação muito mais lenta do que o normal.
2. Algumas ou todas as solicitações dos utilizadores totalmente ignoradas.

Pergunta **10**

Resposta guardada

Nota: 1,0

Quando estás a navegar online, as páginas de internet (websites) podem recolher que informações s

1. A minha localização aproximada online.
2. Que programas utilizo.
3. As minhas preferências, como a língua em que vejo as páginas, em que clico e quanto tempo pass
4. Todas as opções anteriores.

Limpar a minha escolha

◄ Announcements

Ir para...

B.4 EXEMPLO DO FEEDBACK DISPONIBILIZADO APÓS RESPOSTA AO QUESTIOÁRIO

Iniciada	Monday, 19 de July de 2021 às 20:26
Estado	Terminada
Terminada	Monday, 19 de July de 2021 às 20:34
Tempo gasto	7 minutos 21 segundos
Nota	**5,7** num máximo de 10,0 (**57**%)

Pergunta **1**

Correta

Nota: 1,0 em 1,0

Qual das seguintes opções pode levar à disseminação de um programa malicioso?

1. Manter o antivírus atualizado.
2. Utilizar apenas software que foi verificado para a presença de vírus.
3. Utilizar um dispositivo USB de uma fonte desconhecida para trocar dados.
4. Abrir apenas anexos onde foi verificada a presença de vírus e de fontes conhecidas.

A resposta está correcta.

A resposta correta é:
Utilizar um dispositivo USB de uma fonte desconhecida para trocar dados.

Pergunta **2**

Parcialmente correta

Nota: 0,3 em 1,0

A sabotagem de computadores:

1. acontece por ação deliberada de um utilizador.
2. pode envolver o uso de malware, como bots, worms, vírus e outros spywares.
3. pode passar por permitir o acesso indevido aos equipamentos ou eliminar informação.

Pergunta **3**

Parcialmente correta

Nota: 0,3 em 1,0

Qual das afirmações é verdadeira quando se fala de ataques de engenharia social?

1. Utilizam a manipulação emocional dos utilizadores.
2. O objetivo pode ser interromper ou corromper dados para causar danos.
3. O objetivos pode ser a obtenção de objetos de valor como informações, acesso ou dinheiro.
4. Todas as opções anteriores.

A resposta está parcialmente correta.

Sugestão de leitura:

Designa-se por engenharia social, o processo de tentar convencer alguém de algo fictício, usando interaçõ formas: mensagens de correio eletrónico, interações através das redes sociais ou mesmo chamadas telefón

É atualmente, considerada um dos maiores riscos de segurança das pessoas e das organizações. As técnica mais sofisticadas e a vítima muitas vezes não tem a devida noção do ataque.

Link de leitura sugerido:

https://www.cncs.gov.pt/engenharia-social/

https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

A resposta correta é:
Todas as opções anteriores.

Pergunta **4**

Correta

Nota: 1,0 em 1,0

Como podes melhorar a tua segurança online?

1. Utilizar autenticação de duas etapas para aceder às tuas suas contas.
2. Configurar alertas, para que cada vez que se acede de um novo dispositivo a uma conta, sejas not
3. Utilizar palavras pass exclusivas para cada conta online e atualizá-las periodicamente.
4. Todas as opções anteriores.

A resposta está correcta.

A resposta correta é:

Pergunta **5**

Incorreta

Nota: 0,0 em 1,0

O que é a autenticação mutifator?

1. Utilizar algo mais que a senha para entrar numa conta (ex: mensagem com um PIN).
2. Método que permite o acesso a uma conta sem senha.
3. Método de autenticação onde basta que um dos dados fornecidos esteja correto para permitir o a
4. Método de autenticação que não permite a utilização de dados biométricos como a impressão dic reconhecimento da iris.

A resposta está incorreta.

Sugestões de leitura:

Com a verificação em duas etapas ou autenticação mutifator, é uma camada extra de segurança para o cas
Com a verificação em duas etapas ativa, o login na conta é feito com algo que se sabe (como sua senha), e
telemóvel).

Link de leitura sugerido:

https://www.microsoft.com/pt-pt/security/business/identity-access-management/mfa-multi-factor-authent

https://www.cncs.gov.pt/autenticacao-de-2-fatores/

A resposta correta é:
Utilizar algo mais que a senha para entrar numa conta (ex: mensagem com um PIN).

Pergunta **6**

Incorreta

Nota: 0,0 em 1,0

Qual dos seguintes não é considerado "alteração de dados sem permissão"?

1. Alterar o montante de dinheiro numa conta bancária.
2. Acesso a material de computador sem permissão.
3. Escrever um vírus para destruir dados.
4. Nenhuma das opções anteriores.

A resposta está incorreta.

Sugestões de leitura:

Pergunta **7**

Incorreta

Nota: 0,0 em 1,0

O que é roubo de identidade?

1. Quando alguém usa informações de identificação pessoais de outras pessoas sem permissão, com crimes.
2. Quando um utilizador é reencaminhado para uma cópia fraudulenta de um website legítimo.
3. Ocorre quando não são adotadas medidas de segurança suficientes para efetuar pesquisas na Inte
4. Ocorre quando um utilizador utiliza o nickname de outro para se registar num chat.

A resposta está incorreta.

Sugestões de leitura:

Os ladrões de identidade geralmente procuram obter informação pessoal como senhas, números de identi crédito ou CPF.

Os casos de roubo de identidade devem ser imediatamente denunciados às autoridades, bem como outro A Polícia Judiciária tem competência para investigar crimes relacionados com utilizações abusivas de redes

Link de leitura sugerido:

https://www.eset.com/br/furto-identidade/

https://www.avg.com/pt/signal/identity-theft

https://apav.pt/publiproj/index.php/52-projeto-proteus-apoio-a-vitimas-de-furto-de-identidade-e-fraude-

A resposta correta é:
Quando alguém usa informações de identificação pessoais de outras pessoas sem permissão, cometendo f

Pergunta **8**

Correta

Nota: 1,0 em 1,0

Sexting é um termo utilizado para se referir à divulgação de conteúdos eróticos e sensuais através o

Porque não deves partilhar qualquer conteúdo que possa ser considerado erótico ou sexual online:

1. Existe o risco de essas fotos se tornaram públicas.
2. Existe o risco de assédio moral, abuso emocional, pornografia de vingança, assédio.
3. Existe o risco de extorsão.

Pergunta **9**

Correta

Nota: 1,0 em 1,0

Dos seguintes, qual não é um sintoma de ataque de DDOS ?

1. Resposta às solicitações de informação muito mais lenta do que o normal.
2. Algumas ou todas as solicitações dos utilizadores totalmente ignoradas.
3. Acesso não autorizado à informação.
4. Todas as opções anteriores.

A resposta está correcta.

A resposta correta é:
Acesso não autorizado à informação.

Pergunta **10**

Correta

Nota: 1,0 em 1,0

Quando estás a navegar online, as páginas de internet (websites) podem recolher que informações s

1. A minha localização aproximada online.
2. Que programas utilizo.
3. As minhas preferências, como a língua em que vejo as páginas, em que clico e quanto tempo pass
4. Todas as opções anteriores.

A resposta está correcta.

A resposta correta é:
Todas as opções anteriores.

◄ Announcements

Ir para...

C

APÊNDICE C -DOCUMENTOS RELACIONADOS COM OS PLANOS DE AULA

C.1 PLANO AULA DE APLICAÇÃO DOS QUESTIONÁRIOS

Plano de aula:

ATITUDES E COMPORTAMENTOS DE RISCO ONLINE DOS ALUNOS

TÍTULO DA ATIVIDADE	IDENTIFICAÇÃO DE ATITUDES E COMPORTAMENTOS DE RISCO ONLINE
AUTOR	Frederico Manuel Ferreira Marques
ASSUNTO	Atitudes e comportamentos dos alunos na Internet.
COMPETÊNCIAS	• Desenvolvimento pessoal e autonomia. • Pensamento crítico. • Conhecimento técnico e tecnológico. • Raciocínio e resolução de problemas.
GRUPO DE IDADES	11 - 15 anos
DURAÇÃO	45-60 minutos
OBJETIVO	Esta atividade tem em vista identificar comportamentos e atitudes de risco nos alunos envolvidos, com o intuído de recolher informação que permita o desenvolvimento de planos de sensibilização adequados ao perfil dos alunos.
DESCRIÇÃO	Os alunos e a população em geral estão cada vez mais tempo online, ficando assim mais expostos a uma diversidade de ameaças cibernéticas. Considerando que os estudos recentes apontam para um grande crescimento do número de ameaças à segurança informática, e que o seu sucesso depende de algum tipo de intervenção humana, torna-se evidente a necessidade de implementar medidas de proteção adequadas. Por isso é essencial que os utilizadores e particularmente os alunos, desenvolvam competências digitais que lhes permitam fazer face a esta realidade. A escola pretende contribuir para o desenvolvimento dessas competências, mas para isso necessita de saber quais os comportamentos e atitudes dos seus alunos. Esta atividade consiste em responder aos questionários sobre os *"Comportamentos de risco em cibersegurança nas escolas"* e *"Atitudes em Relação à Cibersegurança nas escolas"*, com o intuito de identificar lacunas e permitir à escola a elaboração de um plano de intervenção personalizado. A resposta aos questionários é individual e anónima.

FERRAMENTAS	Computador; Internet; Dispositivo móvel
PROCESSO	O autor dos questionários: • Apresentação dos questionários e dos seus objetivos. • Disponibilização dos links de acesso aos questionários. Os alunos: • Aceder e responder aos questionários
LINKS	Questionário de Atitudes em Relação à Cibersegurança nas escolas: https://cyberawarenessk12.limequery.com/788125?newtest=Y&lang=pt Questionário de Comportamentos de risco em cibersegurança nas escolas: https://cyberawarenessk12.limequery.com/148554?newtest=Y&lang=pt

C.2 PLANO AULA PARA AÇÃO DE SENSIBILIZAÇÃO

Plano de aula:

Cidadão ciberseguro

TÍTULO DA ATIVIDADE	RISCOS DE SEGURANÇA ONLINE (COMPORTAMENTOS E ATITUDES CORRETAS DE PREVENÇÃO E COMBATE)
AUTOR	Frederico Manuel Ferreira Marques
ASSUNTO	Riscos de segurança online para Jovens
COMPETÊNCIAS	• Desenvolvimento pessoal e autonomia. • Pensamento crítico. • Desenvolvimento de aprendizagem colaborativa. • Raciocínio e resolução de problemas. • Desenvolvimento de comportamentos e atitudes.
GRUPO DE IDADES	Alunos do 2º e 3º. Ciclo
DURAÇÃO	90 minutos
OBJETIVO	Desenvolver a capacidade de observação. Distinguir situações de risco. Conhecer atitudes corretas de prevenção e combate a incidentes. Intervir criativamente na prevenção. Encorajar a discussão sobre cibersegurança. Conscientizar sobre os riscos de estar online e da divulgação de dados.

DESCRIÇÃO	Os alunos e a população em geral estão cada vez mais tempo online, ficando assim mais expostos a uma diversidade de ameaças cibernéticas. Por isso é essencial que os utilizadores e particularmente os alunos, desenvolvam competências digitais que lhes permitam fazer face a esta realidade. Esta atividade consiste numa sessão de esclarecimentos planeada para 90 minutos focada nas principais ameaças de cibersegurança da atualidade e a forma como estas se propagam e manifestam nos equipamentos. Aborda também as principais soluções técnicas aplicáveis em equipamentos pessoais para proteção e a função de cada uma delas. A última secção aborda os comportamentos e atitudes que devem ser adotados como de forma a prevenir e combater as ameaças de cibersegurança em todas as suas vertentes. A sessão decorrerá com o apoio de uma apresentação e vídeos que depois de visualizados serviram de ponto de partida para troca de experiências entre os alunos e o professor discutindo os comportamentos e atitudes adotados e mais corretos a adotar. No final reserva-se um espaço para a esclarecimento de dúvidas, divulgação dos links do questionário de autodiagnóstico e links com literatura sugerida para os alunos que queiram aprofundar os seus conhecimentos. A resposta ao questionário poderá ser feita no tempo restante da sessão ou sempre que os alunos pretendam reavaliar os seus conhecimentos, sendo as respostas recolhidas utilizadas pelos alunos para avaliar o seu desempenho e o professor avaliar a eficácia da ação, e identificar áreas que requerem atenção adicional.
FERRAMENTAS	Computador; Projetor; Colunas; Ligação á internet;
PROCESSO	O professor: O professor apresenta o tema expondo as principais problemáticas da atualidade decorrentes da utilização da tecnologia e da internet. Apresenta recorrendo a uma apresentação, imagens, vídeos e outros recursos as principais ameaças, as soluções técnicas disponíveis, e principalmente os comportamentos e atitudes de prevenção e combate ao cibercrime que devem ser adotados para minimizar os riscos. No final o professor disponibiliza tempo para duvidas e discussão do tema. Disponibiliza link de resposta ao questionário de autodiagnóstico. A avaliação das respostas ao questionário de autodiagnóstico servirá aos alunos para avaliarem os seus conhecimentos e ao professor pela análise das respostas avaliar a eficácia da atividade/aula. Os alunos: Os alunos colocam as dúvidas relacionadas com o tema. Respondem ao questionário de autodiagnóstico (disponível no final da sessão e após).

LINKS	Partilha de informação: https://www.youtube.com/watch?v=_y1nlTKQ3S8 Cyberbullying:https://www.youtube.com/watch?v=asTti6y39xI&ab_channel=GoogleAfrica Sexting: https://www.youtube.com/watch?v=PL57cjJlp7g Antivírus: https://www.youtube.com/watch?v=kVUYDI0TI7Q Resumo: https://www.youtube.com/watch?v=SoIpR-kbRcA&t=4s Link para questionário de autodiagnóstico: http://192.168.1.71/moodle
BIBLIOGRAFIA	https://www.apav.pt/cibercrime/ https://www.enisa.europa.eu/media/multimedia/posters/enisa-cyber-poster https://dyn.cncs.gov.pt/pt/boaspraticas/ https://media.rtp.pt/agoranos/artigos/6-regras-fundamentais-para-uso-seguro-da-internet https://www.seguranet.pt/ https://www.tveuropa.pt/noticias/como-ensinar-ciberseguranca-aos-mais-novos/ https://www.curricula.com/security-awareness-training-topics

D E C L A R A Ç Ã O

Declaro, sob compromisso de honra, que o trabalho apresentado neste relatório de projeto, com o título *"Estratégia integrada de avaliação e consciencialização cibernética em contexto escolar"*, é original e foi realizado por Frederico Manuel Ferreira Marques (2190377) sob orientação de Professor Doutor Mário João Gonçalves Antunes (mario.antunes@ipleiria.pt).

Leiria, Novembro de 2021

Frederico Manuel Ferreira Marques

DECLARAÇÃO

Declaro, sob compromisso de honra, que o trabalho apresentado neste relatório de projeto, com o título *"Estratégia integrada de avaliação e consciencialização cibernética em contexto escolar"*, é original e foi realizado por Frederico Manuel Ferreira Marques (2190377) sob orientação de Professor Doutor Mário João Gonçalves Antunes (mario.antunes@ipleiria.pt).

Leiria, Novembro de 2021

Frederico Manuel Ferreira Marques