CIBERSEGURANÇA

GUIA DE BOAS PRÁTICAS PARA AS ESCOLAS

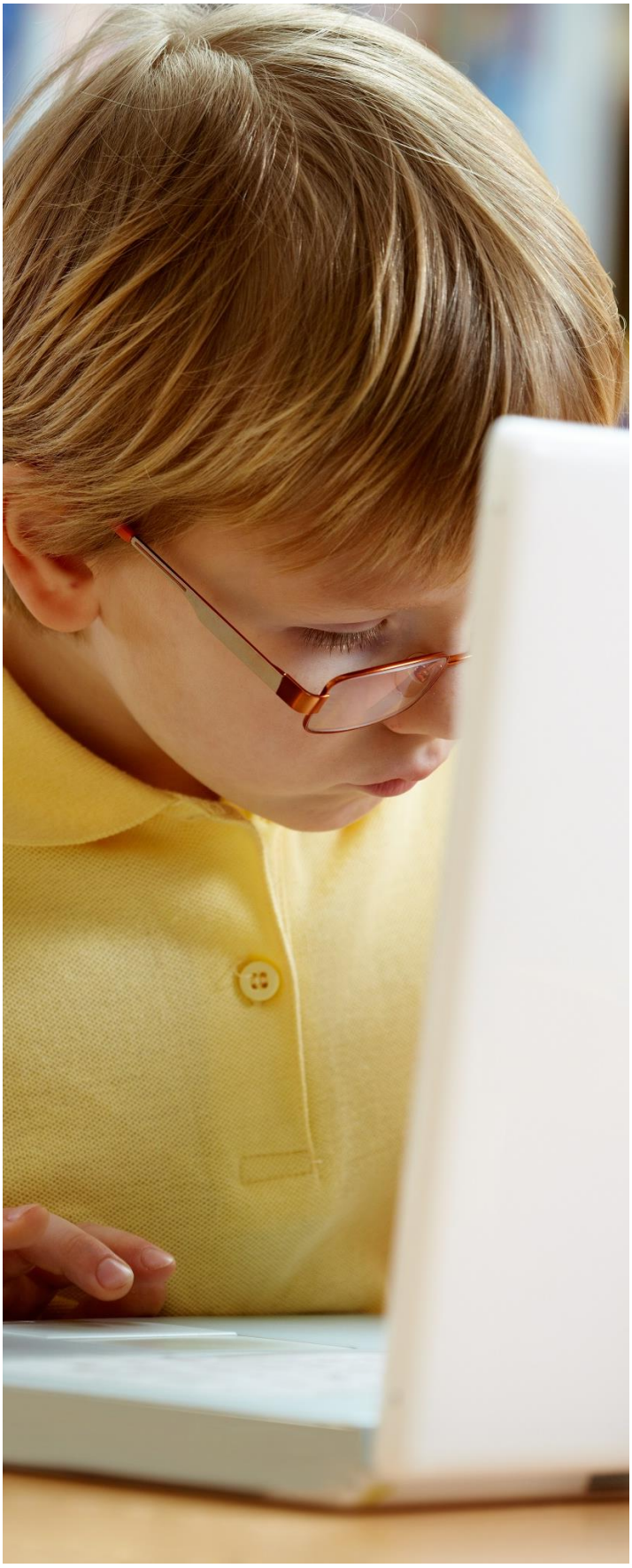
maio, 2024

POLITÉCNICO DE LEIRIA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

No âmbito da tese de Mestrado em Cibersegurança e Informática Forense (MCIF)
Autor: Filipe Bagagem

Este guia de cibersegurança para as instituições de ensino disponibiliza informações e recomendações para auxiliar os Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) de Portugal Continental a protegerem-se no ciberespaço. O guia tem como público-alvo os responsáveis pelas Tecnologias de Informação e Comunicação (TIC) e está dividido em cinco secções. Na primeira secção, são abordados temas gerais da cibersegurança e os principais aspetos que a constituem, tais como os tipos de ataques e os seus impactos. Na segunda secção, o guia apresenta o estado atual da cibersegurança na educação. A terceira secção aborda a legislação e regulamentos em vigor no âmbito da segurança da informação, bem como as normas mais relevantes de cibersegurança. Na quarta secção, são elencadas algumas das recomendações e boas práticas de cibersegurança. Finalmente, são apresentadas as contribuições sobre o tema e as conclusões.

Palavras-chave: Cibersegurança, segurança cibernética, ciberataques, ataques cibernéticos, ciberespaço, espaço cibernético, proteção de dados, governança, proteção de ativos, educação, instituições de ensino, agrupamentos de escolas, escolas não agrupadas, sistemas de informação, tecnologia da informação, segurança da informação, segurança de TI.



SUMÁRIO

Prefácio

Este guia de cibersegurança para as instituições de ensino visa disponibilizar um conjunto de informações e acrescentar valor para se entender melhor o que é a cibersegurança, riscos, potenciais impactos e a necessidade de agir proactivamente para proteger as Tecnologias de Informação e Comunicação (TIC) e os dados contidos nestas.

Prólogo

Este guia teve origem num trabalho académico, mais concretamente numa tese de mestrado de Cibersegurança e Informática Forense ministrada pelo Instituto Politécnico de Leiria, intitulada de "Estado atual da Cibersegurança nos AE/ENA da Região de Leiria" sobe a orientação da Prof. Dr. Marisa Maximiano, do Prof. Ricardo Gomes e o do Prof. Dr. Mário Antunes.

Agradecimentos

Um especial agradecimento a todos os Agrupamentos de Escolas (AE) e Escolas Não Agrupadas (ENA) da região de Leiria que participaram no estudo intitulado de "Estado atual da Cibersegurança nos AE/ENA da Região de Leiria" que serviu de base para elaborar o presente documento.

INTRODUÇÃO

Apresenta-se este guia com o objetivo de promover a conscientização e a compreensão da cibersegurança ou segurança da tecnologia de informação, bem como os possíveis riscos e resultados dos ataques cibernéticos às operações das instituições de ensino. O guia permite visualizar os possíveis riscos, impactos e a necessidade de proteger a infraestrutura tecnológica das instituições de ensino contra ataques mal-intencionados.

A Administração Pública é uma peça fundamental na cibersegurança do país
Não só porque deve dar o exemplo às outras organizações, como porque presta serviços muito importantes para o funcionamento da sociedade, a Administração Pública (e a sua cibersegurança) afeta todos os cidadãos, direta ou indiretamente. Fonte: CNCS

O que é o Guia de Boas Práticas de Cibersegurança para as Escolas?

Este guia de cibersegurança oferece conhecimento às instituições de ensino sobre a cibersegurança, os riscos digitais, os possíveis impactos e a necessidade de uma ação mais proactiva.

A quem se destina este guia?

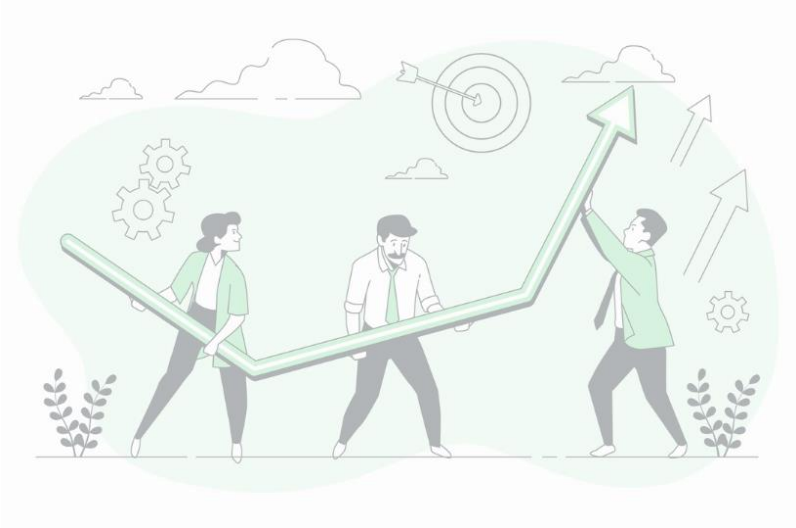
O Guia de Boas Práticas de Cibersegurança para as Escolas é direcionado a vários tipos de utilizadores das instituições de ensino, tais como:

- Direção (Diretor(a), Sub-Diretor(a) ou Adjunto(a) Direção);
- Encarregado de Proteção de Dados;
- Responsável de Segurança;
- Coordenador(a) TIC;
- Técnico(a) Informática;
- Entre outros que assegurem a segurança da informação na instituição de ensino.

Quais são os objetivos deste guia?

Os objetivos do guia são:

1. **Ajudar toda a comunidade Escolar** a proteger-se no espaço digital.
2. **Promover a consciencialização** e compreensão da cibersegurança a fim de assegurar a proteção da informação de cada Escola e a continuidade dos serviços e infraestrutura.
3. **Proporcionar conhecimentos** sobre os possíveis riscos e a adoção de boas práticas de segurança para reduzir a probabilidade de ciberataques, bem como minimizar os impactos que podem advir de um incidente de segurança.



Como está organizado o guia?

O Guia de Boas Práticas de Cibersegurança para as Escolas está segmentado em cinco secções, que servem de orientação para os **dirigentes** das instituições de ensino e os **gestores** e pessoal técnico responsável pelas Tecnologias de Informação e Comunicação (TIC) das instituições de ensino.

De seguida, é apresentado um sumário executivo, que contém a estrutura com os elementos que são abordados ao longo do documento.

SUMÁRIO EXECUTIVO

A tecnologia é uma realidade que faz parte de diversas áreas, tanto na vida profissional como na vida pessoal de cada um de nós. É indiscutível, que o desenvolvimento destas tecnologias está em constante evolução, vão continuar a surgir novos sistemas, novas plataformas, num mundo que vive intensamente a transformação digital.

Neste contexto, as instituições de ensino não são uma exceção. A transformação digital na educação é uma realidade que nos rodeia já há algum tempo, não só pela quantidade de sistemas digitais disponíveis no meio, mas também pelo interesse de toda a comunidade escolar em utilizar a tecnologia, privilegiando a qualidade, a acessibilidade e a simplicidade do acesso à informação.

Contudo, esta transformação digital impõe alguns desafios aos utilizadores e aos responsáveis pelas Tecnologias de Informação e Comunicação (TIC) na instituição de ensino, porque está a atrair cada vez mais cibercriminosos.

Este guia tem por finalidade consciencializar os decisores e responsáveis pelas soluções TIC das instituições de ensino que é necessário passar à ação, de modo a mitigar as principais vulnerabilidades dentro deste contexto. Em termos temáticos, o guia divide-se em cinco capítulos principais:

- "Cibersegurança, ameaças e impactos", onde se apresentam as definições bem como alguns dos tipos de ataques que provocaram mais problemas às organizações portuguesas no último ano;
- "A cibersegurança na Educação", através do qual é apresentada a composição do ecossistema existente nas instituições de ensino, a situação atual sobre a cibersegurança bem como os desafios que as instituições têm de enfrentar;
- "Legislação", engloba os conceitos afetos à governança e que se aplica às entidades e organismos da Administração Pública;
- "Recomendações e Boas Práticas", através do qual são apresentados alguns aspetos que as instituições de ensino podem ter em consideração para melhorar a sua presença no ciberespaço.

Por fim, são apresentadas as principais conclusões através de uma análise global e de um conjunto de destaques com os dados mais relevantes.

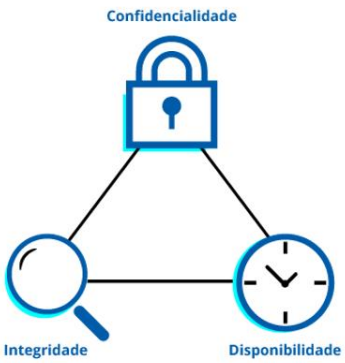
1. CIBERSEGURANÇA, AMEAÇAS E IMPACTOS

O que é a cibersegurança?

A Cibersegurança é uma área de atuação bastante ampla com aplicação não só limitada às tecnologias da informação, mas também à componente dos processos e das pessoas (utilizadores), uma vez que estes são também potenciais vetores de ataque e exploração de potenciais vulnerabilidades com técnicas, como por exemplo a Engenharia Social.

A cibersegurança pode ser definida como um 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.

A segurança da informação assenta sobre três pilares (Figura 10), habitualmente designados por CID (Confidencialidade, Integridade e Disponibilidade) ou CIA (Confidentiality, Integrity and Availability) em inglês, acrónimo que representa as três bases Confidencialidade, Integridade e Disponibilidade.



Quais os tipos de ataques e as suas consequências?

Um ataque cibernético é uma tentativa maliciosa e deliberada de um indivíduo ou grupo de indivíduos violarem o sistema de informação de outro indivíduo ou organização. Existem vários tipos de ataques cibernéticos [1], uns mais conhecidos do que outros, que têm como objetivo causar falhas no serviço, extorquir dinheiro, obter informações com motivações políticas, ou, em casos mais extremos, danificar sistemas com o pretexto de criar o pânico.

Deste modo, seguem abaixo, alguns dos ciberataques mais comuns que acontecem no dia a dia no ciberespaço.

Malware - um malware, ou software malicioso, é um termo genérico que descreve qualquer programa ou código malicioso que seja prejudicial para os sistemas [2]. Alguns dos exemplos são: Adware, Spyware, Vírus, Worms, Trojan, Ransomware, Rootkit, Keylogger, Criptomineração Maliciosa, Exploits, entre outros. Destes, os mais conhecidos são:

- **Trojan** (cavalo de tróia), parece que é algo útil de forma a enganar o utilizador, mas quando entra no sistema, consegue obter acesso não autorizado ao sistema em causa e roubar informações financeiras ou até instalar outras ameaças.
- **Ransomware**, bloqueia o acesso a um dispositivo e/ou cifra os ficheiros existentes no sistema e, normalmente, é exigido o pagamento de um resgate para a devolução da chave que foi utilizada para cifrar os dados. Atualmente, é a ameaça mais comum dos atacantes, uma vez que implica um pagamento em criptomoeda, cujo rasto é difícil de seguir.

Phishing - é um tipo de ataque onde são aplicadas técnicas de engenharia social para obter informação sensível de uma vítima através de um e-mail [3]. O atacante que utiliza este tipo de ataque procura ludibriar os recetores de e-mails para que estes disponibilizem informação sensível através do clique em anexos e/ou URL maliciosos ou da partilha de dados em páginas fraudulentas. Para o efeito, o atacante falseia uma marca credível ou representa alguém de confiança. Quando esta técnica é utilizada através de SMS, dá pelo nome de smishing e, por telefone (voz), de vishing.

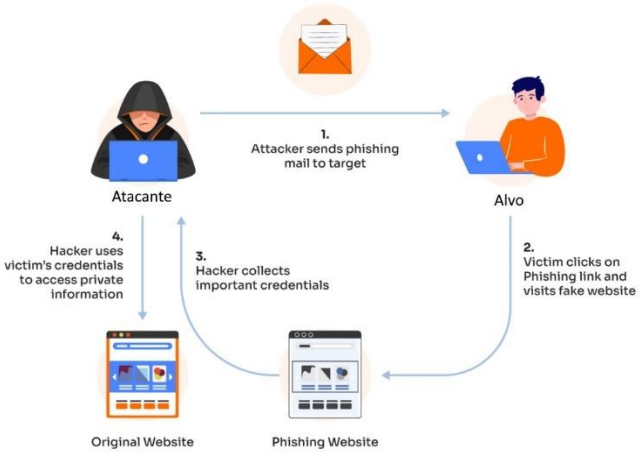
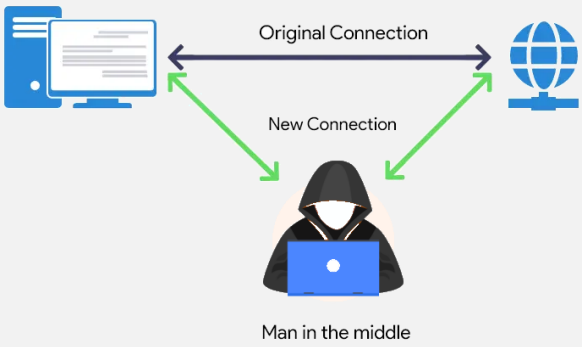


Figura 1 - Ataque de Phishing



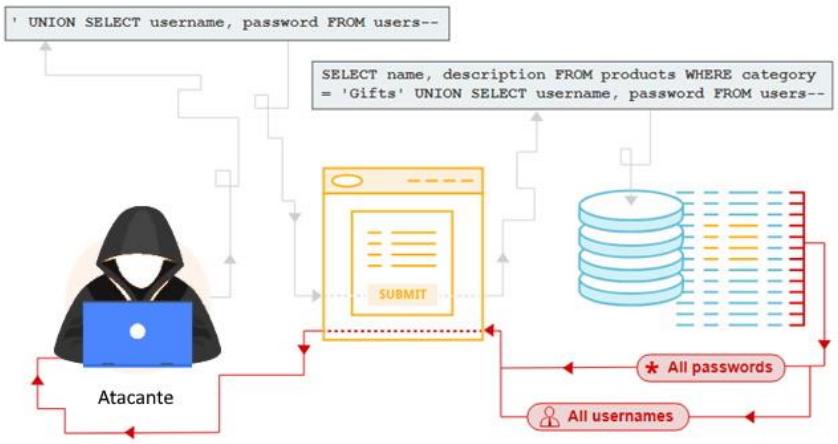
Man-In-The-Middle **(MITM)** - é um tipo de ataque de espionagem, em que o atacante interceta uma conversa existente ou transferência de dados. O atacante consegue infiltrar-se no meio da conversa/transferência, o atacante finge ser ambos participantes legítimos [4]. Isso permite que um atacante intercete informação e dados de qualquer uma das partes, ao mesmo tempo que envia links maliciosos ou outras informações a ambos os participantes legítimos.

***Distributed Denial-of-Service* (DDoS)** - um ataque distribuído de negação de serviço (DDoS) é uma tentativa maliciosa de interromper o tráfego normal de um servidor, serviço ou rede, sobrecarregando o alvo ou a infraestrutura circundante com uma inundação de tráfego de dados [5]. Exemplos destes ataques são o Internet Control Message Protocol (ICMP) flodding (ou smurf attack ou ping of death), o atacante aproveita dispositivos de rede mal configurados e envia pacotes falsificados que executam ping aos computadores da rede de destino. Outro tipo é o SYN flodding, o atacante envia pacotes de SYN para várias portas, mas sem concluir o handshake do Transmission Control Protocol (TCP), fazendo com os que utilizadores legítimos tenham dificuldades no acesso. Um outro tipo é o ataque Denial-of-Service (DoS), em vez de serem várias fontes a realizar o ataque em simultâneo, é apenas uma fonte.

Figura 2 - Ataque de DDoS

Zero-day exploit - Uma exploração de dia zero (também designada por ameaça de dia zero) é um ataque que tira vantagem de uma vulnerabilidade de segurança, para a qual ainda não existe uma correção por parte do fabricante [6]. É chamada de ameaça de dia zero porque, uma vez descoberta a falha, o fabricante/organização tem zero dias para encontrar uma solução.

SQL injection - O SQL injection é uma falha de segurança que permite ao atacante consultar informação de uma ou várias bases de dados de uma determinada aplicação/sistema [7]. Nestes casos, o atacante pode modificar ou apagar informação da base dados, causando assim alterações persistentes no conteúdo ou comportamento da aplicação/sistema.



De seguida são apresentados os ciberataques que causaram mais problemas às organizações, em Portugal, no ano de 2023 [8].

Negação de Serviço Distribuído

O Distributed Denial-of-Service (DDoS) é uma das ciberameaças mais impactantes, causando indisponibilidade dos serviços ou diminuindo o seu desempenho. No ano de 2023, verificou-se que a utilização de Botnets fez aumentar o número de ataques de negação de serviço como também a sua volumetria. Neste mesmo ano, foi reportado o maior ataque DDoS de que há registo, tendo tido como alvo os serviços da Google.

Ransomware

No ano de 2023, verificou-se um crescimento da oferta de serviços do tipo Ransomware-as-a-Service (RaaS). Este modelo de negócio, tornou-se particularmente lucrativo e os grupos cibercriminosos têm-se dedicado cada vez mais a esta atividade tornando este tipo de serviços cada vez mais acessível a qualquer pessoa. Neste mesmo ano, assistiu-se ao uso de uma nova tática de extorsão, onde o ator malicioso ameaça reportar a vítima através das diligências legais, após a mesma ter sido comprometida e não ter reportado às autoridades competentes que tinha sido algo de ataque.

Engenharia Social

A engenharia social foi a técnica de ataque que predominou no ano de 2023. A utilização destas técnicas explora o interesse, a curiosidade, a preocupação e o medo das pessoas, principalmente através da conta de e-mail, para obter informação confidencial, como por exemplo credenciais de acesso. Esta é a técnica favorita dos atores maliciosos para o acesso inicial aos sistemas internos das organizações. Infelizmente, muitos e-mails com conteúdo malicioso, especialmente URLs, ainda passam por mecanismos básicos de segurança de filtragem de e-mails e acabam por ser entregues aos utilizadores.

Tentativa de Login

A tentativa de login continuou a ser um dos ataques mais comuns no ano de 2023. As tentativas de login/ataques de força bruta utilizam a técnica de tentativa e erro para adivinhar a palavra-passe da vítima. Os cibercriminosos utilizam todas as combinações possíveis para obter acesso à conta em questão.

2. A CIBERSEGURANÇA NA EDUCAÇÃO

As novas tecnologias estão cada vez mais presentes nas instituições de ensino. Contudo, esta transformação digital está a atrair cada vez mais cibercriminosos.

De acordo com o último relatório de segurança da CheckPoint, referente ao ano 2023, os setores da educação, governo e saúde continuam a ser os principais alvos de ataques cibernéticos, conforme é possível verificar na Figura 3. O setor da educação/investigação continua a ser o setor mais afetado a nível mundial, com uma média de 2046 tentativas de ataque semanalmente.

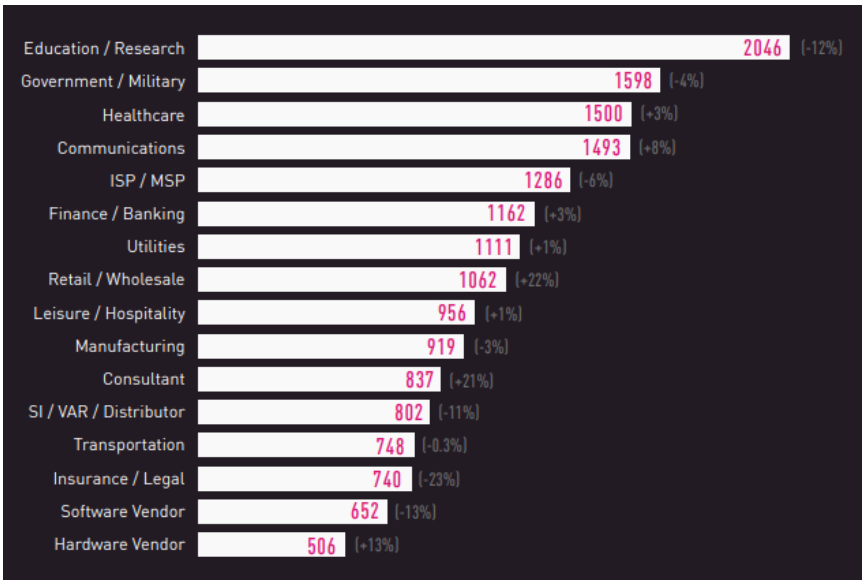


Figura 3 - Média global de ataques semanais por setor em 2023
Fonte: CheckPoint

De acordo com os últimos dados disponibilizados pela Direção-Geral da Educação, apenas 106 Agrupamentos de Escolas (AE)/Escolas Não Agrupadas (ENA) dos 486, obtiveram uma certificação europeia com o Selo de Segurança [9], ou seja, apenas 21,81% das instituições de ensino (AE e ENA) estão a adotar estratégias de sensibilização para uma utilização segura e crítica da tecnologia e dos ambientes digitais.

Ecossistema de uma instituição de ensino cibersegura

O ecossistema de uma instituição de ensino, no âmbito da cibersegurança, é composto por:

- utentes como beneficiários dos serviços e equipamentos;
- plataformas e redes de comunicação que permitem a circulação da informação;
- infraestrutura tecnológica que sustenta toda a atividade da instituição de ensino;
- dispositivos conectados (*Internet of Things - IoT*) e toda a informação gerada e transmitida por estes;
- capacidade de cibersegurança para a proteção dos seus ativos, ou seja, uma solução que protege todos estes elementos.

Qualquer utente da instituição de ensino que tenha acesso a um equipamento (computador e/ou tablet) com sistema de email ou acesso à internet poderá, através de práticas negligentes, infetar toda ou parte da rede interna da instituição com software malicioso. Esta infeção poderá resultar em perda de dados confidenciais, interrupção dos serviços e, claro, prejuízos reputacionais para a instituição de ensino.

3. LEGISLAÇÃO, REGULAMENTOS E NORMAS

O Regime Jurídico da Segurança do Ciberespaço aplica-se aos estabelecimentos públicos de ensino?

Sim, aplica-se!

Nos termos previstos na alínea a) do n.º 1 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto [10], que estabelece o Regime Jurídico da Segurança do Ciberespaço, encontra-se abrangida pelo âmbito de aplicação deste regime jurídico a Administração Pública.

A tipologia de entidades no âmbito de aplicação do Decreto-Lei n.º 65/2021, de 30 de julho [11], que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 [12] do Parlamento Europeu, de 17 de abril de 2019, consta do n.º 1 do artigo 2.º do referido normativo o qual remete para as alíneas a) a d) do n.º 1 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto.

Nos termos do artigo 75.º da Constituição da República Portuguesa, o Estado cria uma rede de estabelecimentos públicos de ensino. De acordo com o enquadramento estabelecido na Lei n.º 46/86, de 14 de outubro, que estabelece a Lei de Bases do Sistema Educativo, respetivamente no artigo 40.º, e nos termos previstos no n.º 1 do artigo 6.º do Decreto-Lei n.º 75/2008, de 22 de abril [13], que aprova o regime de autonomia, administração e gestão dos estabelecimentos públicos da educação pré-escolar e dos ensinos básico e secundário, o agrupamento de escolas é uma unidade organizacional, dotada de órgãos próprios de administração e gestão, constituída por estabelecimentos de educação pré-escolar e escolas de um ou mais níveis e ciclos de ensino.

A Administração Pública integra os agrupamentos de escolas, no âmbito do Ministério da Educação e da Direção-Geral dos Estabelecimentos Escolares, como rede pública de estabelecimentos de ensino, ficando por isso no âmbito de aplicação da Lei 46/2018, de 13 de agosto, e do Decreto-Lei n.º 65/2021, de 30 de julho.

O que é obrigatório cumprir?

Legislação e regulamentos, em vigor, que se aplica às entidades da Administração Pública.

Regulamento Europeu para a proteção de dados pessoais

Estabelece as regras a nível europeu para proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Consultar Regulamento (UE) 2016/679

Normas para a proteção e tratamento de dados pessoais

Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Consultar Lei n.º 58/2019

Orientações técnicas de arquitetura de segurança para a proteção de dados pessoais

Proteção de dados pessoais. Define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes/sistemas de informação e procedimentos a adotar de modo a cumprir as normas do Regulamento Geral sobre a Proteção de Dados (RGPD).

Consultar RCM n.º 41/2018

Regime jurídico da segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148

Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia.

Consultar Lei n.º 46/2018

Decreto-Lei n.º 65/2021, de 30 de julho

Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019. Este normativo define de forma transversal as obrigações relativas a requisitos de segurança e notificação de incidentes. Determina também as competências do CNCS como ANCC – Autoridade Nacional de Certificação em Cibersegurança e estabelece um regime sancionatório para a matéria da certificação e acrescentou um número alargado de obrigações à Administração Pública, com destaque:

- Nomeação de um Responsável de Segurança;
- Identificação dos contactos permanentes;
- Existência de um plano de segurança formal;
- Notificação regular da lista de ativos;
- Realização de avaliações do risco dos ativos;
- Notificação de incidentes;
- Relatório anual.

Consultar Lei n.º 65/2021

Regulamento n.º 183/2022, de 21 de fevereiro

Regulamento que configura instrução técnica relativa à comunicação e informação para cumprimento das obrigações decorrentes do Regime Jurídico da Segurança do Ciberespaço referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes. Este regime jurídico aplica-se às entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação. No Regulamento 183/2022 é possível encontrar os métodos de contacto e a estrutura da informação a ser enviada.

Consultar Lei n.º 183/2022

Quais são as normas de cibersegurança mais populares?

Algumas das *frameworks* de cibersegurança que podem ser adotadas pelas instituições de ensino para melhorarem a sua presença no ciberespaço.

ISO/IEC 27001

A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados de acordo com as necessidades.

Para mais detalhes, consulte a página www.27001.pt

NIST Cybersecurity Framework 2.0

O National Institute of Standards and Technology (NIST) criou uma *framework* de cibersegurança com um conjunto de diretrizes e boas práticas em forma de controlos e ações com o objetivo de mitigar os riscos de segurança da informação nas organizações. A versão mais recente da *framework* da NIST (CSF 2.0) apresenta 6 funções (governar, identificar, proteger, detetar, responder e recuperar) com uma subdivisão em 22 categorias. Para cada categoria existem outras subcategorias com uma variedade de controlos.

Para mais detalhes, consulte a página www.nist.gov/cyberframework

COBIT (Control Objectives for Information and Related Technologies)

Da responsabilidade do ISACA, o COBIT é um referencial de boas práticas para a governação das TIC. Ajuda as organizações a criar valor a partir das TIC e contribui para o equilíbrio entre os benefícios, a otimização dos níveis do risco e a utilização dos recursos disponíveis pelas organizações.

Para mais detalhes, consulte a página www.isaca.org/resources/cobit

CIS Controls Framework

Center for Internet Security Critical Security Controls (CIS Controls) disponibilizou a 18 de maio de 2021, o CIS Control V8, com um conjunto de diretrizes para as organizações melhorarem a segurança dos seus sistemas. Este conjunto de 18 controlos críticos de segurança do CIS fornecem uma estratégia abrangente para proteger os sistemas e redes contra uma variedade de ameaças cibernéticas.

Para descarregar a *framework*, aceda a learn.cisecurity.org/cis-controls-download

Quadro Nacional de Referência para a Cibersegurança (QNRCS)

A segurança do ecossistema de informação depende de todos os seus componentes tecnológicos, das pessoas e dos processos/procedimentos. Neste contexto o Quadro Nacional de Referência para a Cibersegurança (QNRCS) propõe um conjunto de boas práticas/medidas de segurança, concretizadas em exemplos de implementações tecnológicas, processuais ou outras. Estão agrupadas em cinco objetivos de segurança (ver Tabela 1): Identificar, Proteger, Detetar, Responder e Recuperar, com uma ou mais categorias e subcategorias [14]. São identificadas 102 medidas de segurança que abrangem todo o ecossistema de um sistema de informação, do conjunto das quais identificámos as mais relevantes no domínio dos equipamentos/dispositivos (computadores, tablets, impressoras, multifuncionais, smartphones, etc.).

OBJETIVO	DESCRIÇÃO
IDENTIFICAR	Compreensão do contexto da organização, dos ativos que suportam os processos críticos da atividade da organização e dos riscos associados relevantes. Esta compreensão permite que a organização consiga definir e priorizar os seus recursos e investimentos, de acordo com os seus objetivos gerais e com a sua estratégia de gestão do risco.
PROTEGER	Implementação de medidas destinadas a proteger os processos organizativos e os ativos da organização, independentemente da sua natureza tecnológica. Assim, nesta categoria, são definidas medidas orientadas à proteção da organização nas suas três dimensões: Pessoas, Processos e Tecnologia.
DETETAR	Definição e implementação de medidas destinadas a identificar, de forma atempada, os incidentes. Ou seja, a deteção de eventos com um efeito adverso real na segurança das redes e dos sistemas de informação.
RESPONDER	Definição e implementação de medidas de ação apropriadas, em caso de deteção de um incidente. As medidas propostas no âmbito deste objetivo pretendem mitigar o impacto do incidente, ou seja, reduzir os seus potenciais efeitos adversos.
RECUPERAR	Definição e implementação de atividades, que visam a gestão de planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança. As medidas pertencentes a este objetivo pretendem assegurar a resiliência da organização nas suas dimensões: Pessoas, Processos e Tecnologia. E que, no caso de existência de um incidente, a organização consiga utilizar as medidas para suporte à recuperação em tempo útil da sua atividade.

Tabela 1 - Objetivos de Segurança

4. RECOMENDAÇÕES E BOAS PRÁTICAS

Neste capítulo são apresentadas algumas das recomendações e boas práticas que podem ser adotadas pelas instituições de ensino para melhorarem a sua presença no ciberespaço.

#1 SENSIBILIZAR TODA A COMUNIDADE ESCOLAR

Sensibilizar a comunidade escolar (incluindo pais e encarregados de educação) para a adoção das boas práticas de cibersegurança, de modo a aumentar a resiliência da instituição de ensino relativamente às ameaças no ciberespaço. As questões de segurança digital são responsabilidade de todos e, para isso, é necessário sensibilizar toda a comunidade.

Aos funcionários (docentes e não docentes) e colaboradores deve ser ministrada formação mínima no domínio de práticas básicas de segurança da informação e comportamento defensivo.

Abaixo seguem algumas das recomendações do CNCS, literacia e cursos gratuitos, que podem ser divulgados junto da comunidade escolar para promover o conhecimento sobre a cibersegurança.

Sensibilização para adoção de boas práticas
https://dyn.cncs.gov.pt/pt/boaspraticas/

Guia para campanha de sensibilização em 5 passos
https://www.cncs.gov.pt/pt/guia-para-realizar-uma-campanha-de-sensibilizacao/

C-Academy, cursos em formato de e-Learning (MOOCs)
https://www.cncs.gov.pt/pt/cursos-e-learning/

- Cidadão Cibersocial
  https://www.nau.edu.pt/pt/curso/cidadao-cibersocial/
- Cidadão Ciberseguro
  https://www.nau.edu.pt/pt/curso/cidadao-ciberseguro/
- Consumidor Ciberseguro
  https://www.nau.edu.pt/pt/curso/consumidor-ciberseguro/
- Cidadão Ciberinformado
  https://www.nau.edu.pt/pt/curso/cidadao-ciberinformado/

#2 REDIGIR NORMATIVOS SOBRE A CIBERSEGURANÇA

Devem ser definidos normativos, com o objetivo de regular a cibersegurança e a segurança de informação. Estes documentos devem, no mínimo, contemplar os requisitos básicos de segurança da informação na instituição de ensino. Devem, igualmente, ser redigidos numa linguagem acessível, tendo em conta que todos os funcionários (docentes e não docentes) da instituição de ensino devem ter conhecimento dos mesmos. Alguns dos normativos que devem ser do conhecimento da comunidade escolar:

- Política de Segurança Digital: orientações para o uso da internet e dos dispositivos digitais em segurança e como recurso educativo;
- Política de Privacidade e Proteção de Dados;
- Política de Utilização Aceitável (PUA) das TIC – Alunos
- Política de Utilização Aceitável (PUA) das TIC – Docentes
- Política de Utilização Aceitável (PUA) das TIC – Não Docentes

#3 CRIAR PALAVRAS-PASSE FORTES

Quanto mais robusta for a palavra-passe, mais resistente se torna a ataques de força bruta. Crie palavra-passes com, pelo menos, 14 carateres e inclua uma combinação de letras maiúsculas e minúsculas, números e símbolos, se permitido. Uma boa forma de o fazer é criar uma frase de código – utilize uma frase que inclua palavras invulgares ou palavras de diferentes línguas. Além disso, atribua sempre senhas únicas a todas as suas contas online.

O site "Have I been pwned" é um recurso gratuito para qualquer utilizador avaliar rapidamente se as suas credenciais de acesso às plataformas digitais, foram comprometidas ou "exploradas" numa violação de dados.

Verifique se o seu email consta em alguma lista negra
haveibeenpwned.com

Verifique se as suas palavras-passe constam na lista negra
haveibeenpwned.com/Passwords

#4 ATIVAR A AUTENTICAÇÃO MULTIFATOR (MFA)

A autenticação multifator é uma medida de segurança que protege o utilizador e a própria instituição de ensino, exigindo que os utilizadores forneçam dois ou mais fatores de autenticação para aceder a informação confidencial que está alojada nas Tecnologias da Informação (TI), como aplicações, websites, email, entre outros. Esta autenticação adiciona camadas extra de segurança, com o objetivo de dificultar a atividade dos cibercriminosos, uma vez que as palavras-passe podem ser fracas, roubadas, expostas ou vendidas por terceiros. O utilizador apenas conseguirá aceder à informação se apresentar com sucesso duas ou mais provas (ou fatores) de autenticação.

Estes fatores são:

- Conhecimento: algo que só o utilizador sabe. (por exemplo, palavra-passe);
- Posse: algo que só o utilizador tem. (por exemplo, telemóvel);
- Inerência: algo que só o utilizador é. (por exemplo, impressão digital).

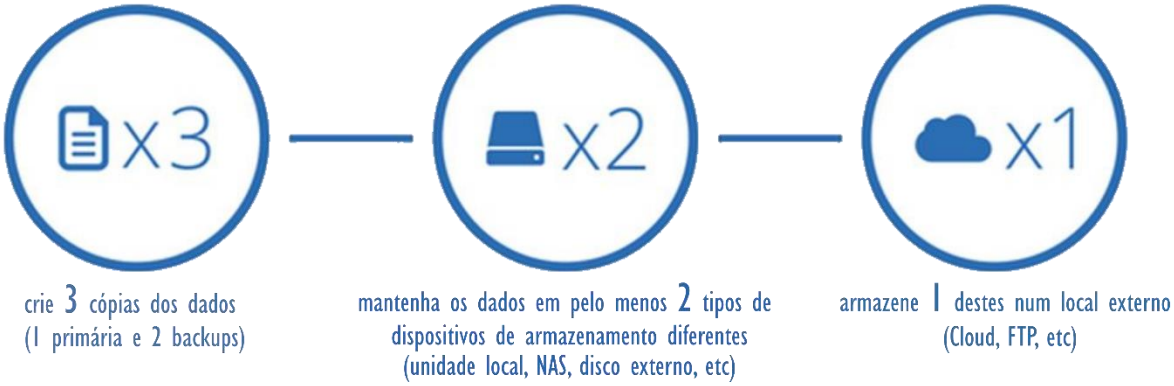
#5 UTILIZAR UM GESTOR DE PALAVRAS-PASSE

Um gestor de palavras-passe é uma forma conveniente e segura de proteger as credenciais de acesso. O gestor permite criar palavras-passe fortes e mantêm-nas em segurança. Sempre que possível a base dados do gestor de palavras-passe deve ser armazenada localmente e deve ser evitado o alojamento na *cloud*. Existem vários gestores de palavras-passe, uns Gratuitos (**G**) e outros Pagos (**P**). **Alguns dos gestores de palavras-passe:**

- KeePass/KeePassXC **(G)**
- LastPass **(G,** plano pessoal**)**
- NordPass **(G,** plano pessoal**)**
- Bitwarden **(G,** plano pessoal**)**
- Dashlane **(P)**
- 1Password **(P)**
- Enpass **(P)**
- Keeper **(P)**

#6 A IMPORTÂNCIA DOS BACKUPS

Para proteger os dados de ataques de *ransomware*, é importante criar e manter uma estratégia de cópias de segurança robusta. A regra 3-2-1 aumenta consideravelmente as possibilidades de recuperação de dados perdidos ou corrompidos.



O 3 significa que devem ser realizadas três cópias de qualquer arquivo. O 2 indica que as cópias devem ser mantidas em dois tipos de armazenamentos diferentes. E o 1 significa que uma das cópias deve ser armazenada num local externo, para evitar que um ataque de *ransomware* a possa afetar.

Outras recomendações:

- Submeter as cópias de segurança periodicamente a testes de integridade e recuperação;
- Cifrar as cópias de segurança para garantir a confidencialidade, só o utilizador com acesso à chave que foi utilizada para cifrar os dados terá acesso à informação protegida;
- Realizar cópias de segurança das configurações dos sistemas críticos;
- Automatizar os sistemas de cópias de segurança e recuperação, garantindo a eficiência e solidez do seu funcionamento;
- Realizar regularmente cópias de segurança da informação crítica para suportes *offline*. De preferência, devem ser realizados backups totais para aumentar a possibilidade de recuperação total dos dados.

#7 IMPLEMENTAR SISTEMA CENTRALIZADO DE MONITORIZAÇÃO DE LOGS

A monitorização de *logs* de sistema é de extrema importância na gestão da segurança de sistemas de informação. Os *logs* são registos detalhados de atividades que ocorrem em sistemas, redes, aplicações e dispositivos. Para uma visão centralizada dos *logs* é recomendado a utilização de uma plataforma de Gestão de Informações e Eventos de Segurança, em inglês Security Information and Event Management (SIEM). Estas plataformas permitem recolher e processar um grande volume de dados e detetar possíveis incidentes e iniciar uma resposta rápida a ameaças, assim como estar em conformidade com requisitos regulatórios.

Alguns dos dados que é importante recolher, pelo menos dos sistemas mais críticos:

- Tipo de evento;
- Identificação do utilizador;
- Protocolo de comunicação;
- Data, hora e fuso horário;
- URL;
- IP de origem e destino;
- Porto de origem e destino;
- Código de sucesso ou falha;

Esta informação permitirá não só identificar ataques ou tentativas de ataques, mas também diagnosticar eventuais problemas nos sistemas. Deverão ser consideradas as obrigações legais quanto ao cumprimento do Regulamento Geral de Proteção de Dados (RGPD).

Plataforma SIEM gratuitas: Elasticsearch, Wazuh, OSSIM, OSSEC, Sagan, Splunk Free, Snort, ELK Stack, entre outras.

#8 MANTER OS SISTEMAS ATUALIZADOS

Com uma boa política de atualizações é possível evitar muitos incidentes de segurança. Não é recomendado utilizar equipamentos com sistemas operativos descontinuados porque os fabricantes deixaram de disponibilizar atualizações de segurança para corrigir vulnerabilidades que, entretanto, foram identificadas. Daqui podem resultar perdas de dados confidenciais, interrupção dos serviços e, claro, prejuízos reputacionais para a instituição de ensino.

QUAL A DIFERENÇA ENTRE A ANÁLISE DE VULNERABILIDADES E O *PENTEST*?

Primeiramente uma vulnerabilidade é um ponto fraco presente num ativo ou num controlo que pode ser explorado por uma ameaça. Podem potencialmente causar um incidente indesejado, que pode originar danos a um sistema, indivíduo ou organização.

A análise de vulnerabilidade pode ser definida como o processo de avaliação e identificação de falhas e potenciais ameaças à segurança de uma infraestrutura tecnológica. Assim, o resultado da avaliação será uma lista com as principais ameaças, organizadas de acordo com a gravidade ou criticidade em relação ao negócio da organização.

Já o *Pentest* (teste de intrusão), envolve o processo de identificação da vulnerabilidade juntamente com a tentativa de explorá-la e simular um ataque real. O objetivo é testar os mecanismos de defesa dos sistemas e mapear os possíveis caminhos que um possível atacante iria seguir.

Uma das principais diferenças entre a análise de vulnerabilidade e o *pentest* está na relação entre a abrangência e a profundidade. Sendo a primeira mais ampla e procura identificar o maior número de riscos possíveis, sem necessariamente analisar a fundo cada um destes riscos.

#9 IDENTIFICAR E MITIGAR VULNERABILIDADES NOS SISTEMAS

As instituições de ensino devem assumir uma postura mais proativa no domínio da identificação, avaliação, priorização e mitigação de vulnerabilidades de software e sistema que podem ser exploradas por atacantes. O objetivo é reduzir o risco de um ciberataque bem-sucedido e manter a informação confidencial segura.

O Catálogo de Vulnerabilidades pode ser utilizado durante o processo de avaliação das vulnerabilidades, e está disponível para consulta no Anexo B do Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança do CNCS.

Algumas das soluções tecnológicas para realizar a análise de vulnerabilidades:

- OpenVAS
- Nessus Vulnerability Scanner
- Nikto
- Shodan
- Entre outros

#10 REALIZAR TESTES DE INTRUSÃO (*PENTEST*)

O *Pentest* é um tipo de avaliação de segurança que envolve a simulação de um ataque cibernético a um sistema, rede ou aplicação web para identificar falhas e avaliar a segurança de um sistema, além de medir a maturidade de segurança da instituição de ensino. Os tipos mais comuns de testes de intrusão, são:

- ***Pentest* externo**: este tipo de teste concentra-se no ataque aos sistemas e infraestrutura externa da instituição. Alguns dos exemplos será o website institucional, o moodle, e as restantes soluções expostas ao público (internet);
- ***Pentest* interno**: este tipo de teste simula um ataque dentro da rede da instituição, para avaliar se os sistemas internos têm falhas nas suas configurações;
- ***Pentest* em Aplicações da Web**: este tipo de teste tem por objetivo explorar as aplicações web da instituição, como formulários online, páginas de login e outros elementos interativos.
- ***Pentest* a redes sem fios (Wi-Fi)**: este tipo de teste concentra-se em atacar as redes sem fios da instituição, como pontos de acesso Wi-Fi e dispositivos Bluetooth;
- ***Pentest* de rede**: este tipo de teste explora a infraestrutura de rede da instituição, como *routers*, *switches* e *firewalls*.

Os testes de intrusão devem ser executados apenas por profissionais de cibersegurança, pois requer conhecimento avançado, sendo também necessária uma autorização prévia da instituição.

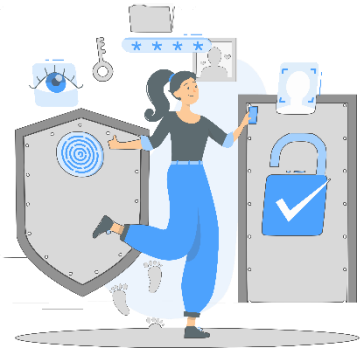
#11 CONTROLAR ADEQUADAMENTE A SEGURANÇA DOS FORNECEDORES

É comum as instituições de ensino recorrerem à subcontratação de serviços de manutenção para os seus sistemas informáticos, pelo que é necessário tomar providências, em sede contratual, junto dos seus fornecedores de Tecnologias de Informação (TI), no sentido de assegurar:

- Cláusulas de confidencialidade;
- A transferência do risco. é necessário atribuir responsabilidades ao fornecedor e aplicar consequências;
- Que as políticas internas também são respeitadas pelos fornecedores, para não comprometer a segurança;
- O Acordo de Nível de Serviço (SLA), assegurando que os serviços contratados são prestados no período acordado.

#12 CONTROLO DE ACESSOS AOS SISTEMAS INFORMÁTICOS

O reforço das medidas de controlo de acesso aos sistemas de informação é algo urgente e deve considerar os utilizadores internos (docentes e não docentes) como os externos (técnicos de informática, fornecedores, entre outros), bem como os utilizadores da instituição de ensino com privilégios máximos, nomeadamente os elementos da direção.



Algumas das recomendações a considerar são:

- Realizar uma correta gestão de palavras-passe;
- Não utilizar contas partilhadas entre utilizadores;
- Restrição de acesso a determinadas redes (VLANs) internas;
- Exigir aos utilizadores a ativação da Autenticação de Multifator (MFA);
- Atribuir privilégios de administração apenas a quem efetivamente necessita;
- Se necessário, os acessos do exterior à rede privada devem ser realizados com recurso a uma VPN (Rede Privada Virtual);
- Restringir o acesso físico a zonas onde se encontram os ativos críticos informáticos vitais para a instituição de ensino.

#13 NOMEAR OS RESPONSÁVEIS PELA SEGURANÇA DA INFORMAÇÃO

Na instituição de ensino deverá existir pelo menos um responsável pela segurança da informação e cabe a este adotar as medidas técnicas e organizacionais que garantam a:

- Salvaguarda das propriedades da informação, designadamente, a confidencialidade, integridade, disponibilidade, autenticidade e o não repúdio;
- Segurança com o tratamento de dados, de modo a prevenir-se contra acessos não autorizados, divulgação não autorizada, modificação, remoção ou eliminação dos dados pessoais.
- Comunicação de incidentes ao CNCS e às restantes entidades competentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do Decreto-Lei n.º 65/2021, de 30 de julho [11].

#14 CRIAR E MANTER ATUALIZADO O INVENTÁRIO DOS ATIVOS

Nos termos do n.º 1 do artigo 4.º no Regulamento n.º 183/2022, de 21 de fevereiro [15], entende -se por «Ativo» todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços. Para cada ativo identificado de acordo com o n.º 1 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho [11], aplica-se o seguinte:

A entidade deve elaborar o inventário dos seus equipamentos de acordo com as seguintes regras:

- Os dispositivos físicos e sistemas devem ser inventariados com a seguinte informação: Número de inventário; Nome e modelo do equipamento; Número de série; e Localização.
- Os dispositivos ligados à rede devem ter a seguinte informação complementar: Endereço IP; e Endereço de hardware.
- Os responsáveis dos dispositivos e sistemas devem ser identificados com, pelo menos, os seguintes elementos: Nome; Contacto; e Departamento.
- Os dispositivos físicos e sistemas devem ser classificados de acordo com a sua criticidade para a entidade.

A entidade deve efetuar o inventário de todas as suas aplicações, identificando:

- Informação necessária ao inventário de uma aplicação, nomeadamente: Nome do software; Versão; e Fabricante.
- Os responsáveis pelas aplicações com, pelo menos, os seguintes elementos: Nome; Contacto; e Departamento.
- A classificação em função da criticidade da aplicação para a entidade;
- Quando aplicável, o tipo de contrato de suporte em vigor com o fornecedor da aplicação ou plataforma de software.

#15 CRIAR E EXECUTAR UM PLANO DE RESPOSTA A CIBERINCIDENTES

Os responsáveis pela instituição de ensino precisam de saber como responder a incidentes de segurança, e como recuperar caso ocorram eventos adversos.

O Plano de Resposta a Incidentes (PRI) deve definir o que a instituição de ensino terá de realizar antes, durante e depois de um incidente de segurança. Este plano deve também incluir quais as funções e responsabilidades dos envolvidos para responder a um incidente.

O PRI deve ser aprovado pelo diretor da instituição de ensino e todos os envolvidos no processo de resposta a incidentes devem ter conhecimento do mesmo. Para uma resposta eficaz o plano deve manter-se sempre atualizado.

As lições aprendidas com os incidentes reais e simulacros permitirão que a instituição de ensino atualize e reforce o seu PRI, bem como as suas políticas, procedimentos e até tecnologias.

#16 CRIAR E EXECUTAR UM PLANO DE AUDITORIAS À SEGURANÇA

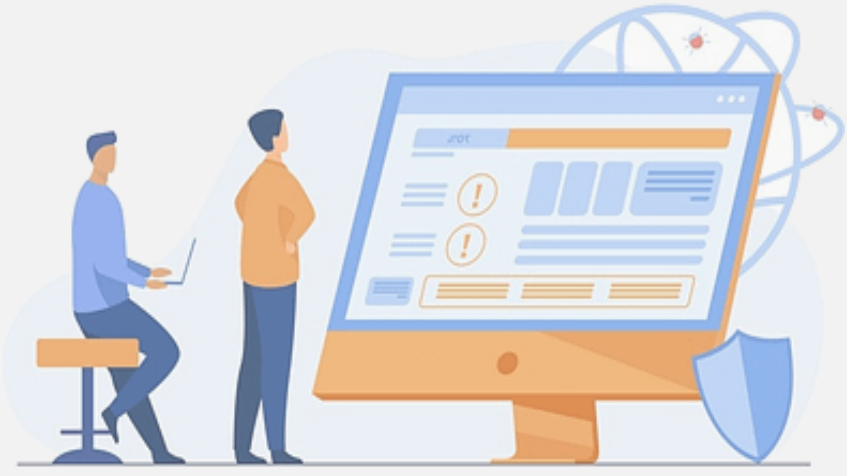
As instituições de ensino devem estabelecer um plano de auditorias à segurança dos sistemas considerados mais críticos para avaliar se os processos, princípios e políticas de cibersegurança estão a ser cumpridos. Existem diversas *frameworks* de Cibersegurança que podem auxiliar, nomeadamente:

- ISO/IEC 27001;
- *Framework* de Cibersegurança do Instituto Nacional de Padrões e Tecnologia Norte-Americano (NIST CSF);
- Controlos do Centro de Segurança para a Internet (CIS);
- Quadro Nacional de Referência para a Cibersegurança (QNRCS).

#17 PROTEGER TODA A INFRAESTRUTURA TECNOLÓGICA

Adotar medidas proativas pode ajudar a proteger adequadamente a infraestrutura tecnológica (equipamentos e sistemas). Seguem algumas das medidas que podem ser adotadas:

- Controlo do acesso à/da Internet - os sistemas internos que estão expostos aos perigos da Internet, podem ser limitados com a configuração de um proxy, permitindo assim a aplicação de medidas restritivas de acesso;
- Configurações e acessos por omissão - para aumentar a robustez das configurações dos equipamentos e sistemas os serviços desnecessários devem ser desativados e as contas de utilizadores por *default* devem ser eliminadas;
- Proteção dos equipamentos terminais - para aumentar a segurança é recomendado instalar e manter atualizado os sistemas de deteção de intrusão, como antivírus, o IDS (Intrusion Detection System), o IPS (Intrusion Prevention System) e o HIDS (Host-based Intrusion Detection System).
- Sistemas descontinuados - Desativar por completo os equipamentos que têm sistemas operativos descontinuados pelo fabricante para garantir que não comprometem a restante infraestrutura tecnológica. Se necessário estes equipamentos apenas deverão ser ligados num ambiente isolado.
- Definição de uma política BYOD (Bring Your Own Device) – nos casos em que os utilizadores utilizam os seus próprios dispositivos para acederem aos recursos tecnológicos disponibilizados pela instituição de ensino, devem ter conhecimento e aceitar a política BYOD.



#18 PROTEGER OS DOMÍNIOS (*Registrars*)

Implementar os principais *standards* de segurança nas vertentes **web** e **email** para melhorar a presença da instituição de ensino no ciberespaço.

O serviço de email continua a ser um dos serviços internet mais utilizados nos contextos de uso pessoal, institucional e empresarial. No entanto, o mesmo foi concebido numa lógica de garantia da entrega das mensagens (disponibilidade), mas sem as preocupações de segurança quer com a integridade do conteúdo, quer com a autenticidade do remetente. De facto, o serviço de email é utilizado de forma abusiva diariamente, seja para envio massivo de mensagens não solicitadas, vulgo SPAM, seja para envio de mensagens com remetente falsificado.

Para fazer face a estes e outros problemas, a indústria, através do Internet Engineering Task Force (IETF), tem vindo a promover a adoção de um conjunto de instrumentos com vista a melhorar a segurança do popular serviço de email, de entre os quais se destacam o Sender Policy Framework (SPF), o DomaimKeys Identified Mail (DKIM) e o Domain-based Message Authentication, Reporting and Conformance (DMARC).

Recomenda-se que sejam adotados os standards **SPF**, **DKIM** e **DMARC** em todos os domínios da instituição de ensino.

Para mais detalhes sobre SPF, DKIM e DMARC, consulte a página cncs.gov.pt/pt/recomendacoes-tecnicas/

Onde verificar os domínios das plataformas digitais da Instituição de Ensino: webcheck.pt

COMO REPORTAR UM INCIDENTE?

Para reportar um incidente ou um cibercrime, utilize os seguintes contactos:

- CERT.PT (CNCS)
- Polícia Judiciária unc3t@pj.pt
- Procuradoria-Geral da República cibercrime@pgr.pt

Qualquer incidente deve ser reportado através do formulário online disponibilizado pelo CNCS

https://www.cncs.gov.pt/pt/notificacao-incidentes/

Caso a entidade não tenha a possibilidade de preencher o formulário online, ou se depare com a indisponibilidade deste, a notificação poderá ser efetuada, a título excecional, através dos seguintes contactos:

- cert@cert.pt;
- (+351) 210 497 399;
- (+351) 910 599 284 (24/7)

A notificação de incidentes ao Centro Nacional de Cibersegurança não se substitui à comunicação à autoridade judiciária ou ao órgão de polícia criminal competente quando esses incidentes configurem também um ilícito criminal cujo procedimento penal dependa de queixa ou de acusação particular.

5. CONCLUSÕES

As ameaças cibernéticas são uma realidade atual, que estão às portas de todas as instituições de ensino, à espreita de qualquer vulnerabilidade humana ou tecnológica. Não existem sistemas 100% seguros, porém são muitas as medidas que podem ser adotadas, em cada estabelecimento de ensino, para aumentarem o seu nível de proteção face aos desafios de segurança atuais. É verdade que não chega apenas implementar medidas tecnológicas, é necessário envolver as pessoas para que exista uma vontade inequívoca e um compromisso por parte de toda a comunidade escolar, bem como das empresas que fornecem e prestam serviços às instituições de ensino.

Com este guia, é possível aceder a um conjunto de recurso que visam disponibilizar as bases de conhecimento sobre o tema cibersegurança, muito direcionado ao ensino, mas também são elencadas algumas das recomendações e boas práticas que podem ajudar os responsáveis pelas Tecnologias da Informação e Comunicação (TIC) da instituição de ensino a proteger e a tornas os seus ambientes digitais mais resilientes.

6. REFERÊNCIAS

[1] H. Ahmetoglu e R. Das, «A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions», *Internet Things*, vol. 20, p. 100615, nov. 2022, doi: 10.1016/j.iot.2022.100615

[2] E. Gandotra, D. Bansal, e S. Sofat, «Malware Analysis and Classification: A Survey», *J. Inf. Secur.*, vol. 05, n.º 02, pp. 56–64, 2014, doi: 10.4236/jis.2014.52006

[3] Z. Alkhalil, C. Hewage, L. Nawaf, e I. Khan, «Phishing Attacks: A Recent Comprehensive Study and a New Anatomy», *Front. Comput. Sci.*, vol. 3, 2021, Disponível em: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060. [Acedido: 31 de janeiro de 2024]

[4] D. Javeed, U. Mohammedbadamasi, C. Ndubuisi, F. Soomro, e M. Asif, *Man in the Middle Attacks: Analysis, Motivation and Prevention*. 2020. doi: 10.13140/RG.2.2.22752.81928

[5] A. B. de Neira, B. Kantarci, e M. Nogueira, «Distributed denial of service attack prediction: Challenges, open issues and opportunities», *Comput. Netw.*, vol. 222, p. 109553, fev. 2023, doi: 10.1016/j.comnet.2022.109553

[6] R. Ahmad, I. Alsmadi, W. Alhamdani, e L. Tawalbeh, «Zero-day attack detection: a systematic literature review», *Artif. Intell. Rev.*, vol. 56, n.º 10, pp. 10733–10811, out. 2023, doi: 10.1007/s10462-023-10437-z

[7] V. Abdullayev e Dr. A. S. Chauhan, «SQL Injection Attack: Quick View», *Mesopotamian J. Cyber Secur.*, pp. 30–34, fev. 2023, doi: 10.58496/MJCS/2023/006

[8]. PT, «Relatório Anual PTSOC 2023», *PTSOC - Centro de Operações de Segurança do .PT*, 6 de fevereiro de 2024. Disponível em: https://ptsoc.pt.pt/pt/relatorio-anual-ptsoc-2023/. [Acedido: 6 de março de 2024]

[9] «Selo de Segurança Digital (eSafety Label) 2022 - Escolas Certificadas | Direção-Geral da Educação». Disponível em: https://www.dge.mec.pt/noticias/selo-de-seguranca-digital-esafety-label-2022-escolas-certificadas. [Acedido: 4 de março de 2024]

[10] «Lei n.º 46/2018 | DR». Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384. [Acedido: 31 de janeiro de 2024]

[11] «Decreto-Lei n.º 65/2021 | DR». Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988. [Acedido: 31 de janeiro de 2024]

[12] «Regulamento (UE) 2019/ do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança)».

[13] «Decreto-Lei n.º 75/2008 | DR». Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/75-2008-249866. [Acedido: 6 de março de 2024]

[14] «cncs-qnrcs-2019.pdf». Disponível em: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf. [Acedido: 31 de janeiro de 2024]

[15] «Regulamento n.º 183/2022». Disponível em: https://files.diariodarepublica.pt/2s/2022/02/036000000/0003400039.pdf. [Acedido: 21 de fevereiro de 2024]

Outras referências:

CHECK POINT: 2024 Cyber Security Report
https://resources.checkpoint.com/cyber-security-resources/2024-cyber-security-report

.PT: Relatório Anual PTSOC 2023
https://ptsoc.pt.pt/wp-content/uploads/2024/02/Relatorio2023_PTSOC_PT.pdf

ENISA: Foresight 2030 Threats
https://www.enisa.europa.eu/publications/foresight-2030-threats

ENISA: Threat Landscape 2023
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

CNCS: Observatório de Cibersegurança, Relatório Riscos e Conflitos de 2023
https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

CNCS: Ciber(in)segurança
https://www.cncs.gov.pt/docs/1ciberin.pdf

CNCS: Ciber-higiene e boas práticas de cibersegurança
https://www.cncs.gov.pt/docs/2ciberhig.pdf

CYBER READINESS INSTITUTE: Recursos para partilhar
https://cyberreadinessinstitute.org/starter-kit/starter-kit-posters/

METARED: Gestão de Passwords
https://eventos.metared.org/file_manager/getFile/106364.html

Índice Remissivo:

CIBERSEGURANÇA

GUIA DE BOAS PRÁTICAS PARA AS ESCOLAS

Autor:
Filipe Bagagem

maio, 2024

Créditos

As imagens utilizadas no presente guia foram obtidas em
FREEPIK.COM
(https://www.freepikcompany.com/freepik)

POLITÉCNICO DE LEIRIA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO