PLANO DE CIBERSEGURANÇA DO AECC

EDD – Equipa Desenvolvimento Digital AECC

julho 2024

"*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*."

Estratégia Nacional de Segurança do Ciberespaço
Resolução do Conselho de Ministros n.º 92/2019, de 5 junho.
Diário da República n.º 108/2019, Série I de 2019-06-05, páginas 2888 – 2895
Presidência do Conselho de Ministros

I – INTRODUÇÃO

No âmbito do Plano Estratégico do Projeto Educativo 2022-2025 do Agrupamento Escolas Coimbra Centro (AECC), Linha de Ação 2 – PRESTAÇÃO DO SERVIÇO EDUCATIVO, 2.1 Oferta educativa e gestão curricular, Campo de Análise, no campo Autonomia e Flexibilidade Curricular, são referidas as seguintes metas a alcançar: "promover a capacitação digital da comunidade educativa; fomentar o uso de ferramentas, plataformas e aplicações digitais na prática letiva." (Projeto Educativo 2022-2025, p. 29, 30).

O novo Plano de Ação de Desenvolvimento Digital de Escola (PADDE) é elaborado num ambiente cada vez mais digital e é crucial que o AECC desenvolva e consiga encontrar um equilíbrio entre o uso dos recursos digitais e a sua segurança.

A navegação feita através de *tablets*, *smartphones,* computadores, portáteis e outros dispositivos informáticos, acedendo a *sites, emails* e *software* digitais escondem riscos e ameaças que muitas vezes são desconhecidos. A segurança durante a navegação *online,* o uso de aplicações e plataformas é algo que passa por boas práticas e parâmetros de proteção, devendo assim ser trabalhada em vários níveis, desde a segurança das redes físicas e dos aplicativos até a educação do utilizador.

O presente documento pretende sensibilizar a comunidade educativa em torno da cibersegurança, tentando dificultar a ação de cibercriminosos, potenciando o uso responsável da *Internet*, dos dispositivos móveis e dos ambientes virtuais.

As normas de conduta e políticas de segurança devem ser seguidas por todos, como forma simples e eficaz de melhorar a proteção da identidade *online* e *offline*, de cada um e dos equipamentos informáticos.

II - OS PRINCIPAIS RISCOS DA INTERNET

Exemplos de ações que os cibercriminosos tentam fazer através da *Internet*:

- → **Atacar sistemas ou equipamentos** - Os sistemas operativos podem estar vulneráveis e serem espiados/observados ou bloqueados para exigir resgates.
- → ***Ciberbullying*** - Uso da *Internet* para praticar ofensas e humilhações a alguém, de forma repetida.
- → **Corromper informações** – Adulterar, mudar o conteúdo original de documentos.
- → **Difamação, injúria e calúnia** – Publicar e/ou difundir informações falsas, ofensas ou acusações maldosas sobre uma pessoa.
- → **Discriminação** - Publicação de mensagens/imagens/vídeos preconceituosos (com referência à cor, etnia, religião, entre outros).
- → **Falsa identidade** – Mentir sobre nome, idade, estado civil, género, etc. para prejudicar uma pessoa.
- → **Roubar informações / *Phishing*** - Mecanismos através dos quais é possível capturar credenciais e palavras-passe únicas, utilizadas para proteger/aceder a contas.
- → **Roubar identidade** - Crime em que alguém se apropria de informações pessoais, geralmente com a intenção de cometer uma fraude/abuso de identidade.
- → **Roubar dinheiro –** Roubo de dados de acesso a contas bancárias para movimento de valores.
- → **Vender dados pessoais** - Comercialização de informações para fins que vão além da finalidade anteriormente pretendida no momento da coleta e que ocorre sem o consentimento do titular.
- → **Plágio** - Copiar algum texto completa ou parcialmente, sem dar os devidos créditos, ou sem a autorização do autor.

III – REGRAS GERAIS DE CIBERSEGURANÇA

3.1 - Palavras-Passe: o primeiro passo para a segurança

As palavras-passe são um dos principais pontos da segurança na *Internet* para impedir o acesso de estranhos às suas contas na rede ou dispositivos.
Regras a seguir:

- → A palavra-passe é secreta e nunca deve ser partilhada.
- → Use palavras-passe diferentes para os seus equipamentos e contas.
- → Evite guardar as palavras-passe nos *browsers.*
- → Use combinações para deixar as suas palavra-passe mais seguras: combine no mínimo 12 carateres, que devem conter pelo menos:
    - uma letra maiúscula;
    - uma letra minúscula*;*
    - um número;
    - um carater especial (exemplos: !, #, $, %, &, ?, ^, ~, (,), [,], @)
    - Exemplo: *Segura20.23!*
- → Crie palavras-passe longas (frases-chave), pelo menos 12 caracteres, e não use termos pessoais como nome, cidade onde nasceu, ou termos conhecidos, como 1234 e *qwerty*[1].
- → Se possível, ative a autenticação de múltiplo fator (Exemplo: para entrar na sua conta, além da *password*, é enviado um código para o telemóvel ou *email*.)
- → Altere as palavras-passe imediatamente caso suspeite que a sua segurança tenha sido comprometida
- → Mude de palavra-passe periodicamente.
- → Altere a palavra-passe de origem na compra de um dispositivo (exemplo: palavra-passe associada à instalação do *Wi-Fi* doméstico).

Se pretender, pode guardar as suas palavras-passe num Gestor de palavras-passe (exemplo: *KeePass; Buttercup*)
Ter uma palavra-passe forte e robusta é fundamental para proteger a informação pessoal.

[1] Sequência de seis letras presente na primeira linha do teclado (*QWERTY*).

3.2 - Proteger o computador e outros equipamentos informáticos de ameaças na *Internet*

Os equipamentos informáticos e as informações guardadas nos mesmos, podem ser alvo de cibercrime através de vírus que visam alterar o funcionamento do dispositivo e, assim, remover, danificar ou apagar dados.

- → Cuidado com as aplicações que instala:
  - Opte por aplicações que são disponibilizadas por plataformas reconhecidas;
  - Limite o acesso das aplicações apenas às funcionalidades essenciais ao funcionamento dos seus equipamentos informáticos.

- → Não transfira músicas, vídeos, filmes ou séries *online* de forma ilegal na *Internet*. A grande maioria dos *sites* que oferecem *download* de arquivos contêm vírus que podem infetar o seu computador.
- → Analise com antivírus as *Pen USB/Pen Drive*, cartões de memória e/ou outros dipositivos informáticos antes de executá-los no seu computador.
  O *software* malicioso é frequentemente distribuído através de *Pen Drive* e/ou outros dispositivos *USB*. Este infiltra-se no sistema por meio destes dispositivos e, quando é executado, permite o "roubo" de dados, e até a destruição de conteúdos nos diferentes dispositivos.
- → Ative o bloqueio automático dos dispositivos usando *PIN* ou *password*.
- → Ative e mantenha o antivírus atualizado.
- → Ative o sistema de segurança de redes de computadores *firewall* que é uma importante barreira de defesa, pois permite filtrar o tráfego suspeito na rede.
- → Navegue sempre em *websites HTTPS*. Estes são mais seguros, uma vez que usam certificados para proteger as comunicações entre o servidor e o utilizador e vice-versa.
- → Utilize uma VPN (Rede Privada Virtual) sempre que se ligar a uma *Wi-Fi* pública ou então opte por utilizar os seus dados móveis para aceder à *Internet* em lugares sem *Wi-Fi* doméstico ou profissional.

É muito importante que mantenha ativo e atualizado o antivírus em todos os dispositivos que use para navegar na *Internet*.

3.3 - Transferir e partilhar ficheiros com segurança

Quando se transfere um ficheiro (fotografias, vídeos e/ou documentos) da *Internet* para o nosso dispositivo é importante ter precauções para não executar programas maliciosos:

- → Um antivírus atualizado ajudará a saber se a transferência é segura.
- → Não transfira ficheiros de *sites* suspeitos.
- → Se o ficheiro chegar através de um *email*, verifique se o remetente é de confiança e não o transfira se tiver dúvidas.
- → Tenha cuidado com *links* que apontam para imagens ou vídeos, mas que na realidade são vírus. Evite transferir ficheiros que terminam em: .exe, .scr, .bat, .com ou .pif, a menos que tenha certeza do seu conteúdo.
- → Para partilhar documentos em segurança, utilize serviços na nuvem como o *OneDrive*.

3.4 - Email

O correio eletrónico é um meio suscetível a muitos ataques.

Desta forma, para capacitarmos comportamentos de desconfiança, apresentamos a "Regra das 6 desconfianças":

.

- → Abrir apenas *emails* de origem fidedigna.
- → Caso abra um *email* desconhecido, não clicar em nenhum *link* ou anexo, dado que são pontos críticos para a instalação de *software* malicioso.
- → Verificar o endereço e a veracidade dos *emails* conhecidos, mesmo os que são aparentemente conhecidos podem estar comprometidos (devemos estar atentos a pormenores desajustados, como: caracteres diferentes, imagens e/ou outros dados).
- → Não enviar informação sensível/confidencial por *email*, mesmo que o destino seja de confiança, o envio pode ser comprometido por terceiros.
- → Identificar o *SPAM* para que o sistema faça uma seleção prévia. A identificação é a melhor maneira de evitar a receção deste tipo de *email*, potencialmente malicioso.
- → Terminar sempre a sessão quando finalizar a utilização do *email*. Uma sessão por encerrar pode ser acedida por alguém que abra o *browser* posteriormente.

3.5 - Redes Sociais

Outro "ponto crítico" são as redes sociais. Assim, o comportamento a incentivar é a preservação da vida privada.

A taxa de utilização das redes sociais atinge, presentemente, valores bastante significativos e os comportamentos de exposição da vida/dados pessoais continuam a ser fatores críticos a evitar. O furto de identidade, entre outros fenómenos consequentes desta exposição, tem que ser contrariado.

Os 5 procedimentos a seguir nas redes sociais, para incentivar a preservação da vida privada:

- → Não aceitar convites de desconhecidos uma vez que aceitá-los é arriscar uma ligação a alguém com intenções maliciosas.
- → Não facultar o número do telemóvel ou moradas no perfil.
- → Não partilhar locais, imagens de crianças ou dados sensíveis, dado que estes podem, ainda, servir para assaltos, pornografia infantil ou conteúdos *deep fake.*
- → Não partilhar notícias falsas (*fake news)* – verificar sempre a fonte. Em caso de dúvida, apenas fontes reconhecidas devem ser legitimadas.
- → Não clicar em publicações (*posts)* suspeitos – podem ser *phishing.* Estes também existem nas redes sociais (devemos usar as mesmas regras de proteção que usamos para o *email*).

3.6 - Navegação

O comportamento a seguir é o de prevenir a navegação por *sites* maliciosos.
A utilização de *Wi-Fi* pública não é segura, a não ser que use uma VPN, uma vez que é possível ficar exposto a terceiros. Também é necessário ter cuidado com as *Apps* que instala nos seus dispositivos.
Os principais comportamentos corretos para se proteger de *Apps* maliciosas:

- → Usar apenas plataformas reconhecidas para instalação de *Apps*.
- → Verificar as pontuações e escolhas do autor; podem dar-nos indicações sobre a segurança da *App*.
- → Não instalar *Apps* duvidosas, que estejam fora das plataformas conhecidas ou que levantem suspeitas.
- → Denunciar *Apps* fraudulentas, para que outros não sejam vítimas.

3.7 - Uso seguro de dispositivos amovíveis

O *software* malicioso é frequentemente distribuído via *Pen Drive* e outros dispositivos informáticos. Estes infiltram-se no sistema por meio dessas ferramentas e quando são executados permitem que o *software* roube dados e até destrua todo o conteúdo do computador.
Dessa forma, no intuito de evitar tais ataques e disseminar boas práticas de cibersegurança, devem observar-se os seguintes procedimentos:

- → Não usar dispositivos *USB* ou outros tipos de dispositivos amovíveis considerados inseguros.
- → Evitar executar dispositivos *USB*, ou outros, automaticamente no seu computador, *tablet* ou *smartphone*.
- → Para evitar a perda da informação, devem efetuar-se cópias de segurança periódicas (*backup*) para locais seguros, podendo utilizar dispositivos físicos (Exemplos: discos externos, *Pen Drive/ Pen USB)* ou serviços na nuvem *OneDrive*.

3.8- O símbolo de "cadeado" no navegador (*browser*) significa que o *site* é seguro?

Quando se utiliza um navegador (*browser*) e, à esquerda do endereço, aparece o símbolo de identidade do *site* (um cadeado), este indica que o conteúdo da página é transferido de forma segura entre o servidor do *site* e o dispositivo de visualização (computador/ telemóvel).

IV - CIDADANIA DIGITAL

Boas práticas que devem ser comuns a todos os universos da comunidade educativa. A saber:

a) Cumprir a legislação em matéria de direitos de autor/*copyright* e a utilização subsequente de materiais obtidos na *Internet*.
b) Todas as atividades escolares que impliquem o uso da *Internet* devem integrar a apresentação de referências bibliográficas normalizadas.
c) Promover ações dirigidas à comunidade educativa de combate ao *bullying* e/ou *ciberbullying*.

V – BOAS PRÁTICAS DE SEGURANÇA DIGITAL EM CONTEXTO ESCOLAR

Importa observar as regras gerais de Cibersegurança, referidas no capítulo anterior, e adotar procedimentos específicos, tendo em vista a segurança dos utilizadores.

4.1 – Cibersegurança - docentes

No meio escolar, os docentes são os interlocutores privilegiados no processo de ensino, responsáveis pela gestão e coordenação das aulas/sessões. Assim, devem:

- → Cumprir e fazer cumprir as regrais gerais de cibersegurança;
- → Promover nos alunos/formandos um comportamento de utilizador responsável e seguro, incorporando a educação para a segurança *online* no currículo, sempre que possível;
- → Fazer cumprir os procedimentos de segurança específicos na utilização de cada ferramenta de acesso e navegação no ciberespaço;
- → Orientar os alunos no acesso e utilização das aplicações e plataformas digitais adotadas pelo agrupamento;

- → Manter um nível de conduta profissional no uso pessoal da tecnologia, dentro e fora do local de trabalho.

4.2 - Cibersegurança - discentes

O acesso à *Internet* é proporcionado aos alunos/formandos, sempre que possível, e estes deverão utilizá-la de forma responsável observando sempre um conjunto de regras e procedimentos preventivos e defensivos. Devem:

- → Cumprir as regras gerais de utilizador;
- → Utilizar o *email* institucional ou pessoal com a devida identificação;
- → Cumprir as regras de acesso às plataformas conforme as instruções emanadas pelos docentes;
- → Solicitar esclarecimentos sobre dúvidas de utilização segura das plataformas e ferramentas digitais aos docentes;
- → Colaborar com os colegas no uso das ferramentas, aplicações e plataformas digitais adotadas pelo Agrupamento, zelando pela segurança dos mesmos na navegação no ciberespaço.

4.3 - Cibersegurança - pessoal não docente.

O corpo não docente, pela qualidade das funções prestadas, está cada vez mais envolvido na esfera da comunicação e interação digital, quer na sua relação interna, quer com as restantes instituições parceiras de serviço e profissionais.

Perante a digitalização dos serviços, importa estabelecer um conjunto de instruções e orientações que promovam o uso responsável e seguro das tecnologias de informação e comunicação. A saber:

- → Cumprir as regras gerais de utilizador;
- → Utilizar o *email* institucional ou pessoal com a devida identificação;
- → Cumprir as regras de acesso às plataformas conforme as instruções emanadas;
- → Colaborar com os colegas no uso das ferramentas, aplicações e plataformas digitais adotadas pelo agrupamento, zelando também pela segurança dos mesmos na navegação no ciberespaço;
- → Reportar anomalias e situações suspeitas ao/à Diretor(a) e/ou à sua equipa;
- → Envolver-se no domínio digital com sentido ético e deontológico.

4.4 - Cibersegurança - Pais e Encarregados de Educação.

Para bem dos alunos e do processo de ensino e de aprendizagem, caberá aos pais e/ou encarregados de educação ou aos alunos/formandos, quando maiores de idade:

- → Ser um modelo apropriado na utilização racional da tecnologia e na adoção de comportamentos seguros *online*.
- → Identificar mudanças no comportamento que possam indicar que o seu filho ou educando está em situação de risco *online*.
- → Procurar ajuda e apoio da escola, ou de outros órgãos competentes, se os seus filhos ou educandos encontrarem problemas ou preocupações *online*.
- → Acompanhar a utilização da *Internet* por parte das crianças/ jovens. É importante conhecer o uso que estes fazem da *Internet* e com quem interagem. Se necessário, bloquear o seu acesso a algumas plataformas/ conteúdos.
- → Assumir a responsabilidade, pela sua própria consciência e aprendizagem, em relação às oportunidades e riscos decorrentes das tecnologias novas e emergentes.
- → Informar os docentes de situações anómalas que possam comprometer a segurança e privacidade dos seus educandos no acesso às plataformas de ensino e de aprendizagem adotadas.
- → Solicitar esclarecimentos sobre o uso de instrumentos, ferramentas e aplicações, junto dos docentes, sempre que considerem necessário para segurança dos seus educandos.

VI – CONCLUSÃO

Vivemos na era tecnológica e digital sensível a ataques e ameaças à nossa segurança que obrigam à implementação de leis e regulamentações de proteção de dados.

O Regulamento Geral de Proteção de Dados (RGPD) que estabelece o regime jurídico de proteção de dados de pessoas singulares, tanto no que respeita ao tratamento como à circulação dos dados pessoais entrou em vigor em Portugal a partir do dia 25 de maio de 2018.

O Plano de Cibersegurança do AECC pretende estar alinhado com as exigências da situação atual no que respeita à Cidadania e Segurança Digital.

As regras referidas neste Plano têm como objetivo implementar uma cultura de segurança da informação/dados digitais no AECC, pelo que devem ser respeitadas por todos os membros da comunidade educativa.

Toda a comunidade escolar é incentivada a ter uma utilização segura e responsável da *Internet*; os docentes são, também, incentivados a facultar esclarecimentos junto dos alunos e pais/encarregados de educação sobre o assunto.

O Plano de Cibersegurança do AECC está disponível na página *Web* do Agrupamento.

Finalmente, não podemos esquecer que a segurança da informação assenta nos seguintes pilares:

- **Confidencialidade** - garantir que a informação seja alcançada somente pelos responsáveis diretos, impedindo que seja divulgada para outros utilizadores ou entidades não autorizados.
- **Integridade** – garantir que a informação não seja alterada ou excluída sem a devida autorização.
- **Disponibilidade** – garantir que o acesso aos sistemas, dados e serviços seja realizado somente por utilizadores ou entidades autorizadas.
- **Autenticidade** – garantir a identidade de quem envia e/ou recebe a informação.

VII - GLOSSÁRIO

Drive **-** unidade de disco destinada a armazenar dados que podem posteriormente ser recuperados.

Firewall **-** é o sistema informático concebido para proteger uma rede de computadores do acesso externo de utilizadores não autorizados

HTTP **- Protocolo de Transferência de Hipertexto** (*HyperText Transfer Protocol*) é o protocolo de comunicação da *World Wide Web (WWW*)[2]

HTTPS **- Protocolo de Transferência de Hipertexto Seguro** (Hypertext Transfer Protocol Secure) - versão segura do protocolo *HTTP*.

Identidade *offline* – refere-se a uma pessoa da vida real que se apresenta diariamente em casa, na escola ou no trabalho.

Identidade *online* - refere-se a uma pessoa que se apresenta aos outros online.

Rede Privada Virtual (VPN) - é uma rede virtual de comunicação privada que utiliza uma infraestrutura pública de telecomunicações para transmitir dados que são protegidos devido à utilização de técnicas de encriptação.

SPAM - mensagens de correio eletrónico não solicitadas, geralmente enviadas de uma forma massiva e indiscriminada, que podem comprometer o bom funcionamento dos sistemas informáticos.

.

[2] Acedido em 22 de novembro de 2023, em: https://www.cncs.gov.pt/pt/glossario/#linhasobservacao

VIII - REFERÊNCIAS BIBLIOGRÁFICAS

- Imagem da capa, acedida em https://shre.ink/ProtecaoDados.
- Plano de Ação para a Transição Digital. Resolução do Conselho de Ministros n.º 30/2020 de 21 de abril.
- *How Secure Is My Password*? (Acedido em 7/09/2023, em: https://www.security.org/how-secure-is-my-password\).
- NORMAS PARA A APRESENTAÇÃO DE REFERÊNCIAS BIBLIOGRÁFICAS (uc.pt). (Acedido 10/2023, em: https://www.uc.pt/fcdef/documentosbiblioteca/Bibliotecadigital/Normas).
- Centro Nacional de Cibersegurança (CNCS). (Acedido em 30/10/2023, em: https://www.cncs.gov.pt/pt/).
- Centro de Operações de Segurança do .PT (PTSOC). (Acedido em 30/10/2023, em: https://ptsoc.pt.pt/pt/).
- Estratégia Nacional de Segurança do Ciberespaço. (Resolução do Conselho de Ministros n.º 92/2019, de 5 junho. Diário da República n.º 108/2019, Série I de 2019-06-05, páginas 2888 – 2895. Presidência do Conselho de Ministros. Acedido em 30/10/2023, em: https://diariodarepublica.pt/dr/home).
- Porto Editora - Dicionário Infopédia de Siglas e Abreviaturas. Dicionário Priberam da Língua Portuguesa (DPLP). **(**Acedido em 20/11/2023, em: https://www.infopedia.pt/dicionarios/siglas-abreviaturas/).
- Dicionário Inglês - Português, *Cambridge Dictionary*. (Acedido em 20/11/2023, em: https://dictionary.cambridge.org/pt/dicionario/ingles-portugues/).
- Plataforma NAU - Ensino e Formação Online para Grandes Audiências, Boas práticas de Cibersegurança – os cinco pontos críticos. (Acedido 6/12/2023, em: https://www.nau.edu.pt/pt/2021/11/30/boas-praticas-de-ciberseguranca-os-cinco-pontos-criticos/).
- Segurança na *Internet.* (Acedido em 7/12/2023, em:
- https://edu.gcfglobal.org/pt/seguranca-na-internet/senhas-o-primeiro-passo-para-a-seguranca/1/).
- Dicionário Priberam da Língua Portuguesa. (Acedido em 19/02/2024, em: https://dicionario.priberam.org/wi-fi).
- Plataforma de Cibersegurança *Bughunt*. (Acedido em 02/2024, em: https://blog.bughunt.com.br/principios-da-seguranca-da-informacao/).
- Plataforma NAU – Bullying e Ciberbullying: Prevenir & Agir. (Acedido em 11/07/2024, em https://www.nau.edu.pt/pt/curso/bullying-e-ciberbullying-prevenir-agir/)

Aprovado em Conselho Pedagógico de 22 de julho de 2024.