Plano de Cibersegurança do AEMM

Direção AE Mem Martins

ÍNDICE

INTRODUÇÃO

Desde a declaração do estado pandémico que se assiste a uma crescente utilização das tecnologias de informação e comunicação no âmbito das relações interpessoais, sejam de cariz subjetivo ou profissional.

Março foi tempo de confinamento, o processo de ensino-aprendizagem foi repensado, as sessões não presenciais, de matriz síncrona e/ou assíncrona, cobriram o plano educativo. Pais, alunos e professores reinventaram os quotidianos em função de restrições e de óticas @ distância.

As escolas convocaram sinergias para que os processo educativos se materializassem em plataformas digitais, assegurando a continuidade das funções da escola e a ligação das famílias com as unidades de ensino.

O documento visado surge na sequência do plano de ensino @ distância, colocando o foco pedagógico na comunicação e informação via digital, que se pressupõe a utilização de aplicações e ferramentas de trabalho *on-line*. O ciberespaço adquiriu também valor e qualidade educativa e pedagógica, onde os conceitos de segurança individual e proteção singular e social constituem matéria de preocupação e ação das entidades e autoridades de segurança. As instituições, com base nos princípios de colaboração e cooperação com as organizações de segurança e proteção, passaram a integrar nos seus planos de ação projetos e normativos ao nível da cibersegurança.

I – CONTEXTUALIZAÇÃO, OBJETIVOS E FINALIDADES DE UM PLANO DE CIBERSEGURANÇA

Compromisso

Aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os agentes educativos.

Missão

O presente documento pretende ser um plano de boas práticas no âmbito da utilização das tecnologias de informação em ciberespaço aberto, potenciando o uso responsável e comprometido do regime de ensino @ distância, bem como os diferentes meios de acolhimento e difusão de informação/dados em meio digital *web*.

Visão

Desenvolvimento e difusão de um plano de boas práticas sobre cibersegurança na criação de uma comunidade educativa mais segura e consciente dos riscos inerentes ao ciberespaço.

Valores

Partilha; rigor; inclusão; segurança; compromisso; complementaridade.

Objetivos

a) Sistematizar os conhecimentos e os dados disponíveis sobre comportamentos e tecnologia no âmbito da cibersegurança;

b) Identificar tendências com base na informação sistematizada;

c) Sensibilizar a comunidade em torno da cibersegurança;

d) Contribuir para a construção de modelos de boas práticas.

II – REGRAS GERAIS DE CIBERSEGURANÇA

2.1. Dados, informações e partilhas

(I) Partilhar com cuidado qualquer conteúdo, certifique-se bem se não irá arrepender-se futuramente. Lembre-se que o que acha engraçado e inofensivo hoje, pode já não ser interpretado da mesma forma amanhã. Para além disso, recorde-se que outras pessoas, que não conhece, poderão eventualmente ter acesso ao que publicou.

(II) Ocultar os seus dados pessoais, como o seu nome do meio, o número do cartão de cidadão, a sua morada, data de aniversário, entre outros que possam identificá-lo.

(III) Ao ir de férias, não expor grandes informações. Optar por publicar as fotos apenas aquando do regresso, pois poder-se-á dar ideias aos "amigos do alheio".

(IV) Não compartilhar as compras efetuadas, essa exposição pode atrair atenções que não são desejadas.

(V) Tornar o perfil das redes sociais privado, para que só os conhecidos possam ver a partilha.

(VI) Não reencaminhar e-mails se não se estiver seguro do seu conteúdo.

(VII) Não copiar conteúdos, o famoso *copy-paste*, sem ter assegurado que todas as hiperligações foram eliminadas.

(VIII) Poder-se-á, para maior segurança, consultar conteúdos web em modo privado ou confidencial.

(IX) Não abrir e-mails suspeitos nem aceder a *links* que não ofereçam segurança.

(X) Guardar registo de todas as mensagens recebidas.

(XI) Desaconselham-se vivamente encontros com utilizadores que se conhecem nas redes sociais.

(XII) Não publicar informações relacionadas com outros utilizadores.

2.2. Dispositivos e páginas WEB.

(I) Proteger o dispositivo pessoal. Evitar que as mensagens, fotos e documentos pessoais sejam lidos por pessoas indesejadas protegendo o dispositivo e garantindo o direito à individualidade. Fazer a encriptação dos dados pessoais.

(II) Verificar se na página *web* que está a utilizar aparece o " https://" e não " http://". Se aparecer um cadeado na barra onde se está a navegar, significa que estamos numa página segura.

(III) Mudar as senhas pessoais com regularidade.

(IV) Verificar sempre se o antivírus está ativo e atualizado.

(V) Prestar atenção aos programas que se instalam via *online*.

(VI) Tomar cuidado com as permissões dadas, pois existem aplicativos que permitem aceder aos dados pessoais, resgatando:

localização;
armazenamento de dados e arquivos;
imagens pela câmara;
contas;
Mensagens;
e-mails;
ferramentas;
aplicações;
serviços pagos;
...

III – CIBERSEGURANÇA EM CONTEXTO ESCOLAR

Os regimes de ensino que promovem processos de aprendizagem @ distância começam a ser uma realidade quotidiana entre as comunidades de aprendentes. Os ambientes digitais povoarão as escolas, em que as tecnologias de informação e educação serão as respostas aos sistemas de ensino a vigorar no século XXI.

As potencialidades de inovação e eficiência tecnológica de informação e comunicação se multiplicam, em paralelo encontraremos os perigos crescentes inerentes à exposição digital, em que a segurança adquire foco de interesse e de necessidade, na medida em que o bem-estar individual e social poderão ser alienados.

Os contextos escolares serão o novo campo de trabalho dos investigadores nos campos da cibersegurança, em que alunos, professores e pais e encarregados de educação se equacionam num universo digital de amplificação universal.

Importa observar não só as regras gerais de utilizador como também procedimentos específicos, prevalecendo sempre o princípio das boas práticas com vista a segurança dos interlocutores.

3.1. Cibersegurança para os pais e encarregados de educação.

Em contexto escolar, no caso de regime de aulas @ distância, os pais e encarregados de educação terão, por essência, um papel funcional de supervisores e tutores das ações dos respetivos educandos.

Para bem dos alunos e do processo de ensino-aprendizagem, caberá aos pais e encarregados de educação:

a) Sensibilizar os alunos para cumprimento das regras gerais de utilizador;
b) Promover comportamentos seguros de acesso ao espaço digital pelos seus educandos;
c) Colaborar com os docentes na disponibilização de meios tecnológicos e de informação e comunicação atualizados e seguros.
d) Verificar procedimentos de segurança antes e após o uso da Internet.
e) Informar os docentes de situações anómalas que possam comprometer a segurança e privacidade dos seus educandos no acesso às plataformas de ensino-aprendizagem adotadas.
f) Solicitar esclarecimentos sobre o uso de instrumentos, ferramentas, aplicações... junto dos docentes sempre que considerem necessário para segurança dos seus educandos.
g) Fazer a limpeza do histórico dos navegadores de Internet frequentemente.
h) Utilizar janelas privadas em navegadores de Internet, especialmente em dispositivos não pessoais.
i) Utilizar definições em alta privacidade em navegadores de Internet e em outras aplicações.
j) Desligar a localização do *smartphone* e de outros dispositivos quando a mesma não é necessária.

3.2. Cibersegurança para os docentes.

Na esfera escolar, os docentes são os interlocutores privilegiados no processo de ensino, responsáveis pela gestão e coordenação das sessões, quer em termos pedagógicos quer em termos técnicos.

No âmbito de um regime não presencial com recurso a instrumentos digitais de informação e comunicação, os professores deverão:

a) Promover nos alunos um comportamento de utilizador responsável e seguro.
b) Cumprir e fazer cumprir as regrais gerais de cibersegurança.
c) Manter os encarregados de educação informados das tecnologias a utilizar sob compromisso de salvaguardar os preceitos de segurança.
d) Fazer cumprir os procedimentos de segurança específicos na utilização de cada ferramenta de acesso e navegação no ciberespaço.
e) Orientar os alunos no acesso e utilização das aplicações, ferramentas e plataformas digitais inerentes ao processo de ensino-aprendizagem.
f) Relembrar os alunos de forma sistemática do uso responsável das ferramentas, aplicações e plataformas de aprendizagem.
g) Colaborar com os colegas no uso das ferramentas, aplicações e plataformas digitais adotadas pelo agrupamento.
h) Fazer a limpeza do histórico dos navegadores de Internet frequentemente.
i) Utilizar janelas privadas em navegadores de Internet, especialmente em dispositivos não pessoais.
j) Utilizar definições em alta privacidade em navegadores de Internet e em outras aplicações.
k) Desligar a localização do *smartphone* e de outros dispositivos quando a mesma não é necessária.

3.3. Cibersegurança para os discentes.

Na qualidade de centro do processo de ensino-aprendizagem, os alunos são os sujeitos destinatários do regime não presencial, tornando-os utilizadores frequentes do ciberespaço, o que os coloca em situação de vulnerabilidade se não forem devidamente acauteladas as regras de segurança e proteção.

A comunidade discente deve observar um conjunto de regras e procedimentos preventivos e defensivos em contexto escolar. A saber:

(i) Cumprir as regras gerais de utilizador.
(ii) Utilizar o e-mail institucional ou pessoal com a devida identificação.
(iii) Cumprir as regras de acesso às plataformas conforme as instruções emanadas pelos docentes.
(iv) Solicitar esclarecimentos sobre dúvidas de utilização segura das plataformas e ferramentas digitais aos docentes.
(v) Informar os pais e encarregados de educação de alterações das emissões digitais síncronas ou assíncronas que possam surgir no momento.
(vi) 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.

(vii) Envolver os encarregados de educação e os pais no processo de ensino não presencial com recurso aos meios e tecnologias de informação e comunicação.
(viii) Fazer a limpeza do histórico dos navegadores de Internet frequentemente.
(ix) Utilizar janelas privadas em navegadores de Internet, especialmente em dispositivos não pessoais.
(x) Utilizar definições em alta privacidade em navegadores de Internet e em outras aplicações.
(xi) Desligar a localização do *smartphone* e de outros dispositivos quando a mesma não é necessária.

3.4. Cibersegurança para o pessoal não docente.

O corpo não docente, em particular os assistentes técnicos, pela qualidade das funções prestadas, são cada vez mais envolvidos 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:

(i) Cumprir as regras gerais de utilizador.
(ii) Utilizar o e-mail institucional ou pessoal com a devida identificação.
(iii) Cumprir as regras de acesso às plataformas conforme as instruções emanadas.
(iv) 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.
(v) Cumprir e fazer cumprir as regrais gerais de cibersegurança.
(vi) Reportar anomalias e situações suspeitas à direção.
(vii) Envolver-se no domínio digital com sentido ético e deontológico.
(viii) Fazer a limpeza do histórico dos navegadores de Internet frequentemente.
(ix) Utilizar janelas privadas em navegadores de Internet, especialmente em dispositivos não pessoais.
(x) Utilizar definições em alta privacidade em navegadores de Internet e em outras aplicações.
(xi) Desligar a localização do *smartphone* e de outros dispositivos quando a mesma não é necessária.

CONCLUSÃO

O plano de cibersegurança surge como um documento de referência no âmbito do ensino não presencial e da relação entre a comunidade via ciberespaço.

Em ambientes de regime @ distância, os efeitos da comunicação e transmissão de informação poderão implicar risco de utilização de plataformas, ferramentas e aplicações digitais. Nesse sentido, encontram-se conjuntos de procedimentos gerais e específicos de cada domínio de interlocutores.

A observação das recomendações e orientações reveste-se de primordial importância no circuito *web* de comunicação entre os diferentes agentes da comunidade educativa, fundamentando-se assim a pertinência do presente documento.

REFERÊNCIAS BIBLIOGRÁFICAS

Antunes, M; Rodrigues, B. (2018) - *Introdução à Cibersegurança*. FCA.

Hintzbergen, J. (2018) - *Fundamentos de Segurança da Informação.* São Paulo: Bresport..

Lei n.º 46/2018 de 13 de agosto, Diário da República, 1.ª série — N.º 155 — 13 de agosto de 2018. Lisboa: Assembleia da República.

Pinheiro, P.P. (2020) – *Proteção de Dados Pessoais*. São Paulo: Saraiva Educação.

Aprovação

Conselho Pedagógico de 25 de novembro de 2020.

Presidente do CP, prof. João Caravaca