PLANO
CIBERSEGURANÇA

Escola Básica com Pré-escolar
BARTOLOMEU PERESTRELO

Plano de Cibersegurança

INTRODUÇÃO

A cibersegurança na escola é vital para proteger os alunos, os docentes, os dados escolares e os recursos educacionais contra uma variedade de ameaças cibernéticas. Além disso, promove um ambiente de aprendizagem online seguro e responsável, preparando os alunos para enfrentar os desafios digitais do mundo moderno. Daí a urgência de ser implementado um plano de cibersegurança, por forma a proteger toda a comunidade educativa de ataques informáticos.

I. LEGISLAÇÃO

Toda a estratégia implementada terá de ter em conta as recomendações e os diplomas legais em vigor, designadamente:

- Regulamento (UE) 2016/679, de 27 de abril de 2016.
- Diretiva (UE) 2016/1148, de 6 de julho de 2026.
- Lei n.º 46/2018, de 13 de agosto.
- Decreto-Lei n.º 65/2021, de 30 de julho.
- Regulamento n.º 183/2022, de 21 de fevereiro.

II. EQUIPA DE CIBERSEGURANÇA

A equipa de cibersegurança é constituída pelos seguintes elementos:

- Sílvio Faria, assessor do conselho executivo
- Luís Carneiro, professor de TIC
- Roberto Mendonça, engenheiro informático

III. OS ATIVOS

As redes Wi-Fi disponíveis na escola são as seguintes:

REDE	***FUNÇÃO***	***ACESSO***
ManuaisDigitais	Facultar o acesso à internet aos tablets do projeto manuais digitais	Tablets dos manuais digitais
EBBP	Facultar o acesso à internet aos equipamentos de suporte às aulas.	Portáteis de sala, quadros interativos.
Guest	Facultar o acesso à Internet aos restantes equipamentos que não se enquadram nos pontos anteriores.	Acesso livre.
Eleicoes	Facultar acesso a internet a dispositivos utilizados durantes os processos eleitorais.	Acesso realizado através de palavra-passe facultada dias antes do processo eleitoral e valida até a segunda-feira seguinte ao dia eleitoral.

Exceção: os docentes poderão requisitar o acesso à internet para o seu computador ou tablet. Para tal, terão que se dirigir ao técnico de informática para introduzir as credenciais.

As redes fixas disponíveis na escola são as seguintes:

REDE	*FUNÇÃO*	*ACESSO*
ebbpadm.edu	Facultar o acesso aos serviços administrativos e Conselho Executivo	Secretaria; Conselho Executivo

ebbpesc.edu	Facultar acesso a internet aos PC fixos disponíveis nos gabinetes e salas de aula	Gabinetes de disciplina, salas de informática

IV. REGRAS GERAIS DE CIBERSEGURANÇA

4.1. Dados, informações e partilhas

- 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.
- 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.
- 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”.
- Não compartilhar as compras efetuadas, essa exposição pode atrair atenções que não são desejadas.
- Tornar o perfil das redes sociais privado, para que só os conhecidos possam ver a partilha.
- Não reencaminhar e-mails se não se estiver seguro do seu conteúdo.
- Não copiar conteúdos, o famoso *copy-paste*, sem ter assegurado que todas as hiperligações foram eliminadas.
- Poder-se-á, para maior segurança, consultar conteúdos web em modo privado ou confidencial.
- Não abrir e-mails suspeitos nem aceder a links que não ofereçam segurança.
- Guardar registo de todas as mensagens recebidas.

- Desaconselham-se, vivamente, encontros com utilizadores que se conhecem nas redes sociais.
- Não publicar informações relacionadas com outros utilizadores.

4.2. Dispositivos e páginas WEB.

- 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.
- 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.
- Mudar as senhas pessoais com regularidade.
- Verificar sempre se o antivírus está ativo e atualizado.
- Prestar atenção aos programas que se instalam via online.
- 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.

V. A CIBERSEGURANÇA NA COMUNIDADE EDUCATIVA

Apresentamos quatro conselhos que todos os elementos da comunidade escolar devem observar:

a. Pense antes de clicar:

- Seja no email ou no seu navegador de internet, nunca clique em links ou abra anexos de origem duvidosa.
- Verifique sempre que os domínios dos remetentes dos e-mails que recebe estão relacionados com a entidade que os envia.

- Verifique que os sites a que acede começam por “https//”.
- 90% dos ciberataques começam através de phishing, um crime informático que consiste na distribuição de mensagens de correio eletrónico com ligações para falsos sítios web (instituições bancárias, redes sociais, ou outras), com o objetivo de obter dados pessoais dos utilizadores através de pedidos de atualização.

b. Utilize passwords fortes:

- Idealmente, a sua password deve ser formada por vários tipos de caracteres, como letras (minúsculas e maiúsculas), números e sinais de pontuação.
- Evite incluir nomes, datas e números de documentos.
- Não divulgue a sua password, não a tenha escrita e não use a mesma password para diferentes logins, pois se alguém a descobrir para uma conta, conseguirá ter acesso a todas as outras.
- As passwords “123456”, “password” e “qwerty” são das mais usadas em todo o mundo. São perigosas por serem pouco complexas e bastante comuns.

c. Bloqueie o dispositivo quando se ausentar:

- Nunca abandone o seu dispositivo sem o bloquear, seja o computador, o telemóvel ou o tablet.
- Defina um tempo de bloqueio automático do dispositivo. Assim, mesmo que se esqueça de o fazer, o aparelho bloqueará sozinho ao fim desse tempo (por exemplo, 30 segundos).
- Deixar o dispositivo desbloqueado pode permitir que informações importantes sejam roubadas por terceiros.

d. Não conecte dispositivos desconhecidos

VI. PROCEDIMENTOS PREVENTIVOS PARA COMUNIDADE EDUCATIVA

a. Cibersegurança para os pais e encarregados de educação.

Em contexto escolar, no caso de regime de aulas a 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:

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

b. 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:

- Promover nos alunos um comportamento de utilizador responsável e seguro.
- Cumprir e fazer cumprir as regrais gerais de cibersegurança.
- Manter os encarregados de educação informados das tecnologias a utilizar sob compromisso de salvaguardar os preceitos de segurança.
- 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, ferramentas e plataformas digitais inerentes ao processo de ensino-aprendizagem.
- Relembrar os alunos de forma sistemática do uso responsável das ferramentas, aplicações e plataformas de aprendizagem.
- Colaborar com os colegas no uso das ferramentas, aplicações e plataformas digitais adotadas pelo agrupamento.
- Fazer a limpeza do histórico dos navegadores de Internet frequentemente.
- Utilizar janelas privadas em navegadores de Internet, especialmente em dispositivos não pessoais.
- Utilizar definições em alta privacidade em navegadores de Internet e em outras aplicações.
- Desligar a localização do smartphone e de outros dispositivos quando a mesma não é necessária.

c. Cibersegurança para os alunos.

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:

- Cumprir as regras gerais de utilizador.
- Utilizar o e-mail 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.
- Informar os pais e encarregados de educação de alterações das emissões digitais síncronas ou assíncronas que possam surgir no momento.
- Colaborar com os colegas no uso das ferramentas, aplicações e plataformas digitais adotadas pela escola, zelando também pela segurança dos mesmos na navegação no ciberespaço.
- Envolver os encarregados de educação e os pais no processo de ensino não presencial com recurso aos meios e tecnologias de informação e comunicação.
- Fazer a limpeza do histórico dos navegadores de Internet frequentemente.
- Utilizar janelas privadas em navegadores de Internet, especialmente em dispositivos não pessoais.
- Utilizar definições em alta privacidade em navegadores de Internet e em outras aplicações.
- Desligar a localização do smartphone e de outros dispositivos quando a mesma não é necessária.

d. 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:

- Cumprir as regras gerais de utilizador.
- Utilizar o e-mail 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.
- Cumprir e fazer cumprir as regrais gerais de cibersegurança.
- Reportar anomalias e situações suspeitas à direção.
- Envolver-se no domínio digital com sentido ético e deontológico.
- Fazer a limpeza do histórico dos navegadores de Internet frequentemente.
- Utilizar janelas privadas em navegadores de Internet, especialmente em dispositivos não pessoais.
- Utilizar definições em alta privacidade em navegadores de Internet e em outras aplicações.
- Desligar a localização do smartphone e de outros dispositivos quando a mesma não é necessária.

VII. PROCEDIMENTOS EM CASO DE INTRUSÃO

Caso tenha sofrido ou identificado um incidente de cibersegurança, na escola, poderá reportá-lo à equipa de resposta a incidentes de cibersegurança, seguindo os seguintes passos:

1.º PASSO

Deve procurar perceber o melhor possível o que se passou, bem como o potencial impacto para si ou para terceiros. Caso considere o incidente

suficientemente relevante para si ou para terceiros, deve reportá-lo à equipa de cibersegurança da escola.

Por exemplo:

- Os seus dados foram cifrados e pedem-lhe um resgate para os decifrar – um ransomware?
- Recebeu um email (ou SMS) de phishing ou com tentativa de extorsão?
- Descobriu um website fraudulento que procura captar informação de eventuais vítimas ou realizar burlas?
- Foi vítima de uma burla numa plataforma digital?
- Alguém tomou conta do seu email?
- O seu website ficou indisponível sem nenhuma razão funcional aparente ou apresenta uma imagem diferente da original?
- Algum outro serviço digital que presta ficou indisponível devido a um ataque?
- Ocorreu uma intrusão num sistema seu e o furto de dados sensíveis?

2.º PASSO

Para informar da melhor maneira possível a equipa, deverá procurar saber descrever o incidente com algumas informações, tais como a descrição do que aconteceu, a data de início, os sistemas e/ou pessoas afetados, bem como os ficheiros e/ou URL comprometidos.

Deve reportar o incidente à equipa de cibsersegurança, utilizando os seguintes contactos:

- s.faria@edu.madeira.gov.pt
- luiscarneiro@edu.madeira.gov.pt
- roberto.p.mendonca@edu.madeira.gov.pt
- O contacto telefónico da escola: 291203400

3.º PASSO

Deve seguir as recomendações que a equipa de cibersegurança indicar. Por exemplo, eliminando um email fraudulento, alterando uma palavra-passe de uma conta comprometida, realizando atualizações aos sistemas, entre outras ações possíveis vocacionadas para o tipo de incidente de cibersegurança em questão.

Qualquer anomalia verificada, a equipa de cibersegurança comunicará à equipa responsável da Secretaria Regional de Educação.

CONCLUSÃO

Se todos seguirmos as determinações constantes deste plano, estaremos mais seguros do surgimento de eventuais ameaças cibernéticas, bem como das suas consequências.

UM FUTURO COM HISTÓRIA