Plano de Cibersegurança

Camacha, outubro 2025

Índice

1 – Introdução

No âmbito do projeto Ciber.EDU da Secretaria Regional de Educação/Direção Regional de Educação e no sentido contribuir para a melhoria da resiliência e maturidade em Cibersegurança e segurança da informação da comunidade educativa da Escola Básica com Pré-escolar e Creche Drº. Alfredo Ferreira Nóbrega Júnior produziu-se o presente plano de Cibersegurança que visa primordialmente informar e proteger a comunidade educativa para possíveis ameaças cibernéticas.

2 – Quadro normativo

▪ 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

3 – Constituição da Equipa de Cibersegurança

A equipa de Cibersegurança da Escola Básica com Pré-escolar e Creche Drº. Alfredo Ferreira Nóbrega Júnior é constituída pelo Vice-Presidente do Conselho Executivo e o Técnico de Informática Filipe Coito Mendonça.

4 – Ativos (Rede e acessos)

As redes acesso Wi-Fi na sede e edificio2 são as seguintes:

(1) Rede manuais digitais na sede, (2) rede de apoio aos serviços administrativos na sede, (3) Rede manuais digitais no edifício 2, (4) rede de apoio aos serviços administrativos na sede no edifício 2 e (5) rede apoio nas salas de aulas no edifício2.

(1) Rede manuais digitais na sede com função principal de fornecer acesso a conteúdos para os tablets dos alunos e os pontos de acessos tem 3 redes associadas, a rede ManuaisDigitais protegido por endereços MAC para acesso tablets dos alunos, rede guest que é uma rede aberta para a comunidade escolar e a rede EB23DAFNJ que é uma

rede protegida com um acesso mais restrito. Os pontos de acesso distribuído pela sede estão nos seguintes espaços:

R/C: salas 1.1, 1.3, 1.4, 1.8, 1.12, 1.13, 1.14, 1.15, 1.18, 1.20 (bastidor 4 no corredor perto desta sala), 1.21, 1.25 e um ponto de acesso exterior na parede da sala 1.8. Um total de 13 pontos de acesso com 2 switchs no bastidor 4.

Piso 1: salas 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.8, 2.9, 2.10, 2.11, 2.12, 2.14, 2.15, 2.16, 2.17, 2.18, 2.19(espaço com bastidor 3), 2.20, 2.21, 2.23. Um total de 20 pontos de acesso com bastidor na sala 2.19.

Piso 2: salas 3.12, 3.11, 3.9, 3.8, 3.7, 3.6, 3.5, GIP e Sala de Operações espaço com Bastidor1 e Bastidor2. Um total de 9 pontos de acessos com bastidor 2 na sala de operações

(2) Rede de apoio aos serviços administrativos na sede tem 3 routers a apoiar acesso a dados para consulta pelo funcionário que apoiam os docentes em cada piso. Router para acesso PBX, Router para acesso cozinha. Router para acesso guarita sul. Router para apoio secretaria e utilizado também sempre que ocorre eleições na sede. Router para apoio conselho executivo. Router apoio conservatório de música.

(3) Rede manuais digitais no edifício 2 terá como função principal de fornecer acesso a conteúdos para os alunos, mas ainda esta em fase de conclusão e julgo terá uma configuração idêntica a da sede. O hardware já foi entregue mais falta finalizar montagem e configuração dos switch e firewall. Os pontos de acesso distribuído pelo edifício 2 estão nos seguintes espaços: Sala 0.10, 0.12, 0.13, 1.1, 1.2, 1.3, 1.8, 1.9, 1.10, 1.11 e cantina. Um total de 10 pontos de Acesso.

(4) Rede de apoio aos serviços administrativos na sede no edifício 2 com router na secretaria.

(5) Rede apoio nas salas de aulas no edifício2 com fornecimento WiFi nas seguintes salas: Sala 1.1, 1.2, 1.3, 1.5, 1.6, 1.8, 1.9 e 1,10. Um total 8 router em que a maioria será desativada após ativação da rede dos manuais digitais.

As redes fixas disponíveis na escola são as seguintes:

Na sede existe a (1) rede administrativa, (2) rede escolar, (3) rede sala de aulas. No edifício 2 existe a (4) rede administrativa, (5) rede escolar.

(1) Esta rede consiste dos serviços administrativo, conselho executivo, serviços de reprografia, todo sistema de acesso via cartão em duas guaritas, carregamento de cartão no quiosque, na cantina passar cartão para consumir refeições, serviços administrativos de biblioteca, serviços do gabinete de apoio ao aluno e à família, conservatório de música e espaços de apoio ao docente, tal como openspace de modo a poder imprimir para a reprografia. Um switch para a rede administrativa no bastidor 1 na sala de operações e outro no bastidor 3 na sala 1.19. Outros switches de apoio: secretaria, openspace, biblioteca, sala 3.10 (local de apoio TI) e reprografia (zona apoio TI). A rede tem um servidor de domínio para autenticação de cada turma e fornece serviços de DHCP e servidor de ficheiros.

(2) A rede escolar consiste das 3 sala de informática existes na sede, salas 2.1, 2.4 e 2.6. A rede tem um servidor de domínio para autenticação de cada turma e fornece serviços de DHCP e servidor de ficheiros. Cada sala tem um switch próprio no bastidor 1 sala 1.2 e 2.6 e no bastidor 2 sala 2.4 ambos os bastidores na sala de operações.

(3) Rede sala de aulas fornece 23 espaço na maioria sala de aulas, que são os seguintes: Sala 1.2, 1.12, 1.13, 1.14, 1.15, 1.20, 2.2, 2.3, 2.5, 2.8, 2.9, 2.10, 2.12, 2.14, 2.17, 3.5, 3.6, 3.7, 3.8, 3.9, 3.11, 3.12 e GIP. Existe um switch no bastidor 1 no piso2 e outro no bastidor 3 no piso1 na sala 1.19. Um switch na biblioteca nesta rede com 3 equipamento para pesquisa para alunos.

(4) A rede administrativa é constituída pelos serviços administrativos/reprografia, sala 1.4 (conselho executivo) - espaço onde encontra o bastidor, computador no corredor para os acessos via cartão e ainda os telefones VOIP. Estes estão situados nesta rede nos seguintes locais: sala 1.4 (conselho executivo), sala 1.7 (serviços especializados), Sala 0.2 (serviços administrativos), corredor ao lado do computador de acesso junto a porta da secretaria e cozinha, num total de 5 telefones.

(5) Rede escolar é a sala 1.5 que é a sala de informática, com switch no bastidor 5 na sala 1.4.

5 – Normas gerais de Cibersegurança

- Nunca partilhar os seus dados pessoais, como o seu apelido, o número do cartão de cidadão, a sua morada, data de aniversário, entre outros que possam identificá-lo;

- Optar por um perfil das redes sociais privado, para que só os conhecidos possam ver a partilha;
- Não reencaminhar e-mails sem conhecer o seu conteúdo;
- Não copiar conteúdos, com *copy-paste*, sem eliminar hiperligações;
- Aumentar o nível de segurança, realizando pesquisa de conteúdos na internet em modo privado ou confidencial;

- Desconfiar sempre dos e-mails e nunca aceder a links suspeitos;

- Encriptação dos dados pessoais, favorecendo a individualidade e privacidade;

-Verificar se na página web que está a utilizar é referido 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 e possuir um antivírus ativo e sempre atualizado;
- Condicionar e estar em alerta para a instalação de programas via online;
- Crie a sua password variando os tipos de caracteres, como letras (minúsculas e maiúsculas), números e sinais de pontuação;

- Não incluir nomes, datas e números de documentos;

- Não utilizar a mesma password para várias contas;

- Nunca abandone o seu dispositivo sem o bloquear e defina um tempo automático de bloqueio de forma ao seu dispositivo nunca ficar desbloqueado na sua ausência.

6 – Procedimento em caso de incidente de Cibersegurança

Em caso de incidente de Cibersegurança, tais como:

1) Identificar o incidente(s):

- Roubou do seu e-mail;

- ransomware: Os seus dados foram cifrados e pedem-lhe um resgate para os decifrar;

- phishing: Recebeu um e-mail (ou SMS) de 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;

- 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) Reportar o incidente(s):

Descrever o incidente dando ênfase à cronologia, possível ambiente de "contágio" e ficheiros e/ou URL comprometidos.

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

eb23camachacpn@edu.madeira.gov.pt

filipe.mendonca@edu.madeira.gov.pt

rgpd.ebpeccamacha@edu.madeira.gov.pt

3) Minimizar e/ou extinguir as consequências do incidente

Definição de um plano de ações e recomendações em conjunto com a equipa de Cibersegurança, tais como, eliminação do e-mail "Tóxico", alterações de palavras passe de contas e atualização de sistemas.

Os incidentes de Cibersegurança, serão superiormente comunicados pela equipa de Cibersegurança da Escola

7 - Anexos

7.1 PUA – Politica de uso aceitável

Política de utilização aceitável (PUA)

01 | Objetivo

O objetivo deste documento é definir a utilização responsável dos serviços, recursos eletrónicos e infraestrutura de comunicações da Escola Básica com Pré-escolar e Creche Dr. Alfredo Ferreira Nóbrega Júnior, adiante designada por **EBPEC Dr. AFNJ.**

02 | Procedimento

2.1 Âmbito

- Portais Institucionais e plataformas de backoffice de apoio aos processos da atividade;
- Infraestrutura de comunicações com fios e sem fios;
- Serviço de correio eletrónico;
- Recursos computacionais ligados à infraestrutura de comunicações;
- Acesso a serviços eletrónicos externos, efetuados a partir das redes de comunicações da **EBPEC Dr. AFNJ**;
- Acesso a serviços eletrónicos externos, cujo sistema de controlo de acesso seja através de VPN, utilizando as credenciais da **EBPEC Dr. AFNJ**;
- Trabalho remoto.

2.2 Introdução

A **EBPEC Dr. AFNJ** disponibiliza um conjunto de serviços de rede e eletrónicos com o objetivo de apoiar os processos de ensino/aprendizagem, acesso à informação e comunicação interna e externa.

A utilização de serviços de rede e eletrónicos, deverá ser levada a cabo em estreita consonância com o Regulamento Interno, com o **Plano de Cibersegurança** e os valores da escola. Uma correta utilização contribui, também, para reduzir os riscos de segurança que podem ter um impacto elevado no funcionamento dos mesmos.

As credenciais institucionais (login/password) de acesso aos serviços de rede, plataformas e correio eletrónico, atribuída a cada membro da comunidade escolar, é pessoal e intransmissível, sendo cada indivíduo responsável legal pela sua utilização.

A caixa de correio eletrónico atribuída a cada membro da comunidade escolar deverá apenas ser utilizada para uso institucional, sendo cada indivíduo responsável pela sua correta utilização.

A correta utilização de equipamento eletrónico, propriedade da **EBPEC Dr. AFNJ**, de membros da comunidade escolar, ligados à rede de comunicações da escola, é da responsabilidade legal de cada indivíduo.

A infraestrutura de comunicações da **EBPEC Dr. AFNJ** é constituída por um conjunto de redes internas interligadas entre si e à rede que permite o acesso à Internet.

2.3 Destinatários

- Alunos dos vários ciclos;
- Trabalhadores docentes internos e externos;
- Trabalhadores não docentes internos e externos;
- Outras pessoas com vínculo temporário com a **EBPEC Dr. AFNJ**;
- Utilizadores nacionais ou internacionais credenciados na **EBPEC Dr. AFNJ**.

2.4 Conhecimento da PUA

Os utilizadores que usufruem dos serviços, recursos eletrónicos e infraestrutura de comunicações da **EBPEC Dr. AFNJ** podem consultar a PUA no site da escola.

Os utilizadores, a partir da atribuição das credenciais institucionais de acesso, passam a estar vinculados à política de utilização aceitável expressa neste documento.

2.5 Política de Utilização Aceitável (PUA)

Enquadramento

A Política de Utilização Aceitável (PUA) das Tecnologias de Informação e Comunicação (TIC) da **EBPEC Dr. AFNJ** tem como objetivo estabelecer os princípios orientadores da utilização adequada dos sistemas informáticos e redes de comunicações da escola.

A presente política de utilização aceitável é aplicável a todos os seus docentes, não docentes, formandos, encarregados de educação, parceiros e convidados.

Todos os intervenientes educativos devem estar conscientes da sua responsabilidade aquando do uso dos sistemas informáticos da escola, uso que deve assumir-se inerentemente legal, ético e profissional. Todos devem adotar, dentro do possível, as medidas necessárias para proteger os sistemas de dados e de informação contra acesso não autorizado, danos, perdas, abusos e roubo.

Pressupostos

Os Sistemas de Informação e as TIC incluem as redes, os dados e o seu armazenamento, as tecnologias de comunicação digital online e offline e os dispositivos de acesso. Exemplos: telemóveis, tablets, computadores, câmaras digitais, correio eletrónico, sites e redes sociais.

Os Sistemas de Informação da escola devem ser utilizados de forma adequada, sendo que, ao abrigo da lei portuguesa e das diretivas europeias os seguintes atos constituem uma infração punível por lei: obter acesso não autorizado a material informático, obter acesso não autorizado a material informático com o intuito de cometer ou facilitar outros atos ilícitos ou de alterar material informático sem autorização. Os equipamentos e programas informáticos disponibilizados pela escola só podem ser utilizados para fins relacionados com a escola e para uso educacional.

Geral

1.1 A informação disponibilizada pelos serviços eletrónicos, da qual a **EBPEC Dr. AFNJ** é proprietária ou depositária legal, deve ser utilizada/processada de acordo com a

legislação em vigor dos direitos de autor, da proteção de dados ou outra legalmente aplicável.

1.2 O acesso à informação disponibilizada pelos serviços eletrónicos deve ser realizado em consonância com as permissões atribuídas pela **EBPEC Dr. AFNJ** ao membro da comunidade escolar.

1.3 É da responsabilidade de cada indivíduo reportar o desaparecimento, falta de segurança ou roubo da informação acessível.

1.4 A informação retirada dos serviços eletrónicos existentes pelo membro da comunidade escolar no âmbito da sua atividade, para equipamentos eletrónicos da sua responsabilidade, deve ser protegida e utilizada de acordo com o ponto 1.1. Quando terminar a sua utilização a informação copiada deverá ser eliminada do equipamento eletrónico.

1.5 A utilização de serviços de rede e eletrónicos para fins publicitários só é possível para divulgação de atividades próprias da **EBPEC Dr. AFNJ**.

1.6 Não é permitida a utilização da infraestrutura de comunicações da **EBPEC Dr. AFNJ** para fins comerciais ou, de uma maneira geral, para fins não compatíveis com a atividade institucional da **EBPEC Dr. AFNJ**.

1.7 Não é permitida a instalação de novas infraestruturas de comunicações com e sem fios na **EBPEC Dr. AFNJ**, sem consentimento prévio do Conselho Executivo.

1.8 Os serviços de rede e eletrónicos disponibilizados através da infraestrutura de comunicações da **EBPEC Dr. AFNJ** não poderão ser disponibilizados a terceiros – a título de venda, aluguer ou cedência – pelos Serviços, Unidades Orgânicas ou utilizadores individuais que a ela estejam ligados.

1.9 Em certos casos, e sempre mediante autorização prévia do Conselho Executivo, o acesso poderá ser facultado a terceiros, nomeadamente e apenas quando se trate de instituições do sistema de ensino, ciência, tecnologia e cultura, com as quais a escola tenha protocolo de colaboração.

1.10 A utilização dos serviços de rede e eletrónicos para fins pessoais, só é permitida se tal não conduzir a uma degradação ou inoperacionalidade de meios e serviços, e se tal não representar quaisquer custos adicionais. Em qualquer caso, a utilização para fins pessoais tem sempre menor prioridade que a utilização institucional, reservando-se a **EBPEC Dr. AFNJ** o direito de a interromper.

Segurança

2.1 Os equipamentos ligados à infraestrutura de comunicação da escola, e que são utilizados para acesso aos serviços de rede e eletrónicos, devem estar protegidos contra ataques informáticos (exemplo: antivírus, firewall).
2.2 O utilizador de um equipamento informático ligado à infraestrutura de comunicação da **EBPEC Dr. AFNJ** deve garantir que o mesmo não é abandonado temporariamente sem estar bloqueado com uma password. Caso isso aconteça, está configurado o tempo de inutilização que despoleta automaticamente o encerramento da sessão.
2.3 O utilizador deve garantir que a sua conta institucional de acesso aos serviços de rede e eletrónicos possui uma password com complexidade elevada para reduzir o risco de ser facilmente descoberta. Esta password não deverá nunca ser transmitida a terceiros.
2.4 O utilizador deve assegurar que no momento de introdução da sua password, para autenticação nos serviços de rede e eletrónicos, se encontra resguardado para que terceiros não a possam ficar a conhecer.
2.5 Quando terminar a interação com os serviços de rede e eletrónicos deve sempre ser efetuada a operação de "logout", disponível na aplicação, e de seguida encerrar a mesma (exemplo: browsers para acesso a portais).
2.6 Deve ser evitado, sempre que possível, o acesso aos serviços de rede e eletrónicos da **EBPEC Dr. AFNJ** a partir de equipamentos de utilização pública cuja confiança não possa ser facilmente comprovável (devido à utilização de software malicioso estilo "keylogger" ou outro semelhante).
2.7 No início do ano letivo, as contas de utilizador e e-mail de antigos colaboradores são desativadas. Após período considerado adequado são eliminadas.
2.8 O acesso aos servidores e bastidores da **EBPEC Dr. AFNJ** são restritos ao pessoal autorizado e devem estar sempre fechados à chave.
2.9 As principais palavras-passe de acesso a plataformas da **EBPEC Dr. AFNJ** estão guardadas no cofre da escola.
2.10 Existe uma configuração interna por segmentação de redes e servidores, dividindo a rede professores/colaboradores e rede alunos. A rede wi-fi é isolada destas redes.
2.11 Apenas a o técnico de informática e a Equipa de Cibersegurança têm acesso ao servidor.

Serviço de correio eletrónico

3.1 A caixa de correio eletrónico atribuída a qualquer membro da comunidade escolar é considerada institucional. Deve, por isso, ser utilizada para transmissão oficial de informações ou outras trocas de informação no âmbito da atividade na **EBPEC Dr. AFNJ**.

3.2 A **EBPEC Dr. AFNJ** nunca solicita, por email, telefone ou qualquer outro meio, as credenciais de autenticação (password).

3.3 A caixa referida no ponto 3.1 não pode ser utilizada para fins comerciais ou qualquer outro fim que ponha em causa o bom nome da **EBPEC Dr. AFNJ**.

3.4 A caixa de correio eletrónico atribuída possui uma capacidade limitada, pelo que deverá ser efetuada uma manutenção periódica de arquivo das mensagens, garantindo a operacionalidade permanente da receção de
mensagens institucionais.

3.5 Não devem ser enviadas mensagens para um elevado número de destinatários exteriores. Atualmente existem sistemas externos que, quando esta situação é detetada, colocam o sistema de correio eletrónico da **EBPEC Dr. AFNJ** numa "lista negra", bloqueando o envio de mensagens por parte de todos os endereços da **EBPEC Dr. AFNJ**.

3.6 A abertura de mensagens e de anexos provenientes de endereços de origem desconhecida deve ser evitada, dado este ser um dos meios mais utilizados para a distribuição de vírus, "malware" e "phishing". Sempre que aconteçam estas situações, devem ser comunicadas à equipa de Cibersegurança e ao Técnico de Informática. Posteriormente, devem clicar com o botão do lado direito e denunciar phishing, e depois bloquear e eliminar.

3.7 O serviço de correio eletrónico da **EBPEC Dr. AFNJ** não deve ser utilizado para distribuição massiva de mensagens (SPAM).

3.8 Aquando da receção de emails gerais, não devem fazer "responder a todos", de forma a não enviar emails em
massa desnecessários.

3.9 Ter em atenção que "CC", significa Carbon Copy, e serve para dar conhecimento, ficando todos os destinatários
visíveis.

3.10 Ter em atenção que "BCC", significa Blind Carbon Copy, e serve para dar conhecimento, não ficando os destinatários visíveis.

Restrições

4.1 Não é permitido retirar para o exterior, por qualquer meio eletrónico, informação propriedade da **EBPEC Dr. AFNJ** sem autorização prévia do Conselho Executivo, sob pena de procedimento disciplinar e/ou criminal.
4.2 Não se deve guardar documentos profissionais que contenham informações pessoais ou sensíveis, relacionadas com a escola em todos os dispositivos pessoais (como computadores portáteis, tablets, telemóveis), salvo se estiverem protegidos por palavra-passe ou encriptados.
4.3 Aquando da utilização dos serviços de rede e eletrónicos da **EBPEC Dr. AFNJ** não é permitido:

- Qualquer utilização que seja ilegal de acordo com a legislação Portuguesa;
- Qualquer utilização que impacte no bom nome da **EBPEC Dr. AFNJ** no exterior;
- O consumo continuado de elevada largura de banda, sem autorização prévia;
- Pesquisa não autorizada de vulnerabilidades em equipamentos informáticos, o que inclui, mas não se restringe, a scans automáticos;
- Tentativa ou acesso não autorizado a sistemas internos ou externos à da **EBPEC Dr. AFNJ**;
- Utilização da ligação à infraestrutura de comunicações da **EBPEC Dr. AFNJ** para tentativa de interrupção de serviços ("Denial-of-Service") prestados pela **EBPEC Dr. AFNJ** ou por externos;
- Distribuir, deliberadamente ou por inação, programas que afetem negativamente a atividade de outros utilizadores, quer **EBPEC Dr. AFNJ** quer de redes externas (Vírus, "Spyware", etc);
- Mecanismos que alterem a validade dos dados de endereços físicos de interfaces ("Mac Address Spoofing");
- Falsificação de endereços de hardware de comunicações.

4.4 Qualquer acesso não autorizado aos serviços de rede e eletrónicos disponibilizados pela **EBPEC Dr. AFNJ** é considerado como uso indevido e, como tal, passível de procedimento disciplinar e/ou criminal.

4.5 Qualquer acesso não autorizado a informação pessoal, reservada ou confidencial, é considerado como uso indevido e, como tal, passível de procedimento disciplinar e/ou criminal.
4.6 Não é permitida a disponibilização de conteúdos cuja propriedade é protegida por direitos de autor.
4.7 Não é permitida qualquer utilização de serviços de rede e eletrónicos da **EBPEC Dr. AFNJ** que viole as normas estabelecidas no presente documento ou as disposições legais em vigor, com especial ênfase nas disposições consignadas na lei da criminalidade informática (Lei n.º 109/2009, de 15 de setembro).
4.8 Em trabalho remoto, não é permitido a ligação a redes não seguras/confiáveis (Ex: Wi-fi do café)
4.9 A utilização de VPN para acesso ao servidor da escola só deve ser feita somente com autorização do Conselho Executivo, adotando as mesmas boas práticas aplicáveis ao trabalho presencial.
4.10 Apenas é permitido ligar computadores pessoais à rede por cabo da **EBPEC Dr. AFNJ**, após autorização do Conselho Executivo, e configurados pelo Técnico de Informática da escola.
4.11 O computador da escola serve somente para trabalho no âmbito da atividade da escola, não podendo ser utilizado por terceiros não autorizados (Ex: Utilização pelos filhos, Visualização de filmes, Downloads não autorizados, Jogos, …)

Direito

À **EBPEC Dr. AFNJ** reserva-se o direito de:
5.1 Auditar os serviços de rede e eletrónicos para validar as políticas de utilização definidas.
5.2 Realizar ações de monitorização/auditoria dos serviços de rede e eletrónicos, para efeitos de segurança e manutenção de serviços, por pessoal autorizado e sem colocar em causa a confidencialidade da informação.
5.3 Analisar eventuais denúncias sobre o incumprimento do previsto neste documento. No caso destas terem procedência, as entidades envolvidas serão notificadas devendo, de imediato, regularizar a sua situação. Em casos extremos, e com o fim de evitar danos maiores, a **EBPEC Dr. AFNJ** poderá bloquear, unilateralmente, contas institucionais, caixas de correio, acesso a serviços de rede e eletrónicos ou desligar temporariamente

da infraestrutura de comunicações, o equipamento eletrónico de uma pessoa singular ou coletiva. Em tais situações, a **EBPEC Dr. AFNJ** fará todos esforços para informar as entidades envolvidas antes de pôr em prática as ações descritas anteriormente. Os processos que forem considerados mais críticos serão dados a conhecer ao Conselho Executivo, equipa de Cibersegurança da escola e reportados ainda à equipa de Cibersegurança CIBER.EDU, da Divisão de Tecnologias, Segurança e Infraestruturas / Direção de Serviços de Tecnologias e Ambientes Inovadores de Aprendizagem.

Responsabilidade

6.1 A **EBPEC Dr. AFNJ** não assume qualquer responsabilidade legal pelo uso dos serviços, recursos eletrónicos disponibilizados e da sua infraestrutura de comunicações quando este envolva qualquer atuação contrária à lei ou às presentes normas, recaindo tal responsabilidade sobre os utilizadores.

7.2 Despacho de nomeação da equipa de Cibersegurança

Despacho / Nº16 - 2023/2024

Nomeação de Equipa de Cibersegurança

No âmbito do Plano de Cibersegurança e de acordo com a lei nomeio para a Equipa de Cibersegurança da Escola o Vice-Presidente do Conselho Executivo, o docente Carlos Paulo de Nóbrega e o Técnico de Informática, Filipe Coito Mendonça.

O presente despacho produz efeitos a partir da presente data.

O Presidente do Conselho Executivo

João Daniel Nunes Quintal

03/04/2024

8. Nota final

Documento aprovado em sede de Conselho Pedagógico, no dia 8 de janeiro de 2025 e com obtenção de parecer favorável na reunião ordinária do Conselho da Comunidade Educativa realizada no dia 22 de abril de 2025