2025

2026

Escola Básica e Secundária / PE

Caldas da Rainha

Plano de Cibersegurança

Ciber.EDU

Índice

Índice de Tabelas

Siglas e abreviaturas

DRE – Direção Regional de Educação

DSTAIA – Direção de Serviços de Tecnologias e Ambientes Inovadores de Aprendizagem

DTSI – Direção de Tecnologias, Segurança e Infraestruturas

Escola – Escola Básica e Secundária /PE da Calheta

PUA – Política de Utilização Aceitável

TIC – Tecnologias de Informação e Comunicação

VPN – Virtual Private Network (Rede Privada Virtual)

Termos e Definições

2FA / MFA – Autenticação de dois ou múltiplos fatores: Método de segurança que exige mais do que uma senha para aceder a uma conta, combinando diferentes fatores.

Baiting – Isco digital: Ataque que usa um ficheiro ou dispositivo atrativo para levar o utilizador a executar uma ação perigosa.

Engenharia Social – Manipulação humana: Técnicas usadas para enganar pessoas a revelar informação ou realizar ações que comprometem a segurança.

Hacker – Especialista em sistemas: Pessoa com grandes conhecimentos informáticos capaz de explorar sistemas; pode atuar eticamente ou de forma maliciosa.

Malware – Software malicioso: Programa criado para danificar, explorar ou aceder indevidamente a sistemas informáticos.

Patches – Atualizações de software: Correções que resolvem falhas, melhoram a segurança ou adicionam funcionalidades.

Phishing – Fraude digital: Tentativa de obter dados sensíveis (como palavras-passe) através de mensagens falsas que imitam fontes legítimas.

Pretexting – Ataque com pretexto: Técnica em que o atacante inventa uma história falsa para ganhar a confiança da vítima e obter informações.

Ransomware – *Malware* de resgate: Programa malicioso que bloqueia ficheiros ou sistemas e exige pagamento para restaurar o acesso.

Servidor – Sistema de serviços: Computador ou sistema que fornece serviços, recursos ou dados a outros computadores numa rede.

Trojan (Cavalo de Troia) – Malware disfarçado: Software malicioso que se apresenta como legítimo para enganar o utilizador e executar ações prejudiciais.

Worm – Vermes de rede: Programa malicioso que se propaga automaticamente através de redes sem necessidade de ação do utilizador.

01 | Introdução

A segurança tornou-se um tema cada vez mais relevante nos diversos setores da sociedade, e as escolas públicas não estão imunes a esse desafio. Com a crescente digitalização da educação e a integração de tecnologias no ambiente escolar, a Cibersegurança assume um papel essencial na proteção dos dados pessoais de alunos, docentes, não docentes e demais colaboradores, bem como das informações financeiras, contabilísticas e administrativas. Além disso, é fundamental garantir a integridade dos sistemas e a continuidade das atividades pedagógicas.

O principal objetivo das partes envolvidas é reforçar a infraestrutura tecnológica — incluindo servidores, redes e equipamentos como computadores e dispositivos móveis — e assegurar a proteção dos dados armazenados, tanto em ambientes físicos quanto em nuvens.

Apesar da implementação de mecanismos de prevenção, os incidentes de cibersegurança têm-se tornado mais frequentes e complexos. Nesse contexto, é imperativo preparar a Escola Básica e Secundária / PE da Calheta para elevar o seu nível de cibersegurança, considerando as múltiplas dimensões envolvidas.

A adoção de medidas eficazes de segurança cibernética é crucial para prevenir ataques como o roubo de dados, invasões de sistemas e disseminação de vírus e *malware.* A proteção dos dispositivos e das redes utilizadas na instituição é indispensável para garantir a privacidade e proporcionar um ambiente educacional seguro.

Dessa forma, torna-se necessário continuar a proporcionar os recursos adequados — como equipamentos informáticos atualizados e tecnologias de segurança da informação, além de promover a consciencialização de todos os utilizadores da rede quanto à adoção de comportamentos seguros que contribuam para a prevenção de ataques cibernéticos.

Por fim, importa destacar que a utilização dos sistemas de informação da Escola está sujeita a legislação específica e a diretivas europeias, sendo os infratores responsabilizados civil e criminalmente.

02 | Equipa de Cibersegurança

O responsável de segurança é o elemento de contacto da Escola do ponto de vista técnico/operacional estando em contacto permanente com a equipa Ciber.Edu. É responsável pela operacionalização do Plano, pela implementação de processos de deteção e resolução de incidentes de cibersegurança e de implementação de processos e procedimentos específicos conforme as solicitações da equipa de Ciber.Edu.

A equipa é composta pelos seguintes elementos:

Elemento	Nome	Correio eletrónico	Cargo
1	José Carlos Santos Pestana	carlospestana@edu.madeira.gov.pt	Vice-presidente do Conselho Executivo Responsável da equipa de Cibersegurança
2	Roberto Carlos Rocha Moniz	roberto.rocha@edu.madeira.gov.pt	Técnico de Sistemas de Tecnologias de Informação
3	Maria Luísa Alves Teles	luisateles@edu.madeira.gov.pt	Técnica de Sistemas de Tecnologias de Informação
4	Mariela Sousa da Silva	marielasilva@edu.madeira.gov.pt	Coordenadora TIC
5	Joaquim António Teixeira Rebelo	joaquim.rebelo@edu.madeira.gov.pt	Coordenador do Polo da Fajã
6	Hélder Rogério Carreira Vinagre	heldervinagre@edu.madeira.gov.pt	Coordenador 1.º Ciclo

Tabela 1 - Equipa de Cibersegurança

A Equipa de Cibersegurança foi nomeada pelo Conselho Executivo em 09 de dezembro de 2025.

03 | Identificação de funções ou atividades críticas

A Escola desenvolve um conjunto de atividades que pela sua natureza apresentam potenciais riscos, com níveis críticos diferenciados.

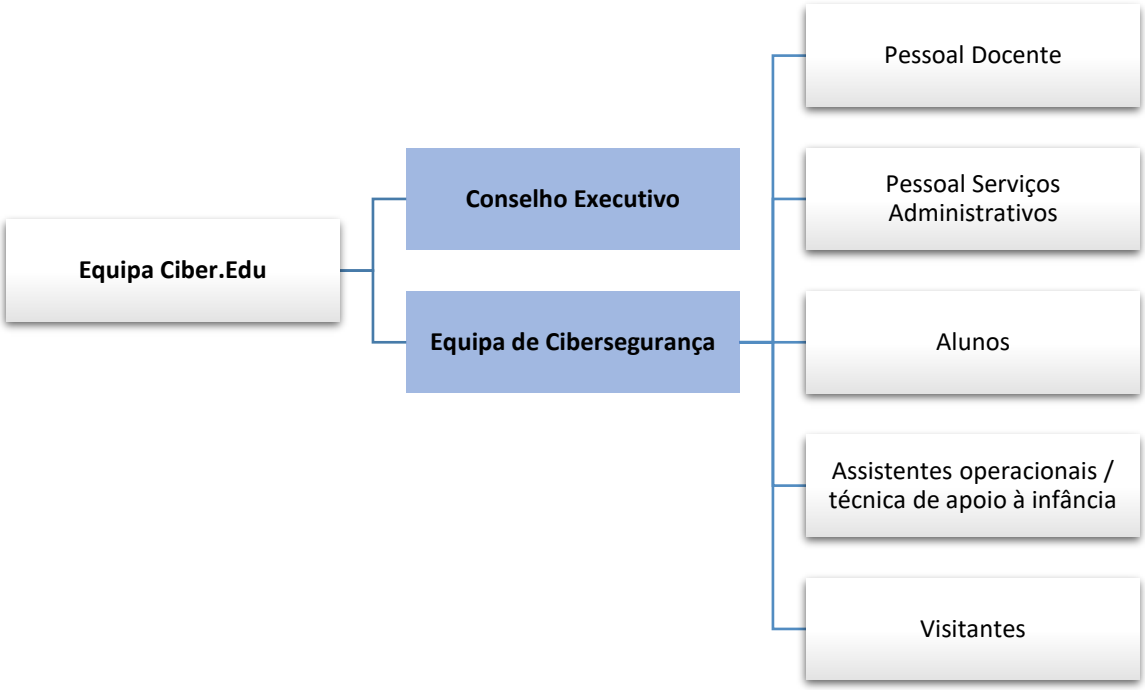
Foram definidos os riscos mais relevantes para a organização que, no quadro abaixo, se encontram ordenados por criticidade, identificação de potenciais ameaças e consequentes impactos, e ainda, identificação de dependências internas e externas entre sistemas.

Anexo A

Tabela 2 – Listagem de atividades críticas da EBS/PE Calheta

04 | Cadeia de Responsabilidade

A cadeia de responsabilidade visa estabelecer uma rede de comunicação que se quer célere e eficaz, entre as equipas Ciber.Edu, Cibersegurança da Escola e a comunidade educativa, para que a atuação, quer na implementação de processos, procedimentos ou medidas, quer na prevenção, resolução ou mitigação do impacto de eventuais incidentes cibernéticos, seja rápida.



05 | Mapa de emergência Cibersegurança

Um Mapa de Emergência de Cibersegurança é um plano detalhado que visa preparar e orientar uma organização em caso de incidentes de segurança cibernética. Este plano descreve as etapas necessárias para responder de forma eficaz a ataques cibernéticos, minimizando o impacto e facilitando a recuperação rápida.

Notificação do Incidente:

Qualquer incidente de segurança cibernética deve ser comunicado a um membro da equipa de Cibersegurança, com preferência para o **elemento 1** – responsável pela equipa de Cibersegurança da Escola. No caso de o incidente ocorrer no Polo da Fajã, poderá comunicar o incidente aos **elementos 5 ou 6** ou **através de formulário próprio.**

Versão: 09/12/2025

1. AVALIAÇÃO DO INCIDENTE:

1.1. Consultar o Plano de Cibersegurança e identificar o tipo de incidente. (Tabela 3)
1.2. Analisar o procedimento a adotar preferencialmente com a colaboração de outros elementos da equipa.

2. RESOLUÇÃO DO INCIDENTE:

2.1. Consoante o incidente, proceder de acordo com os procedimentos previstos.

3. RECUPERAÇÃO DO INCIDENTE:

3.1. Após resolução do incidente, será necessário averiguar os danos causados pelo mesmo.
3.2. E procedimentos necessários para restaurar o normal funcionamento do Sistema

4. REGISTO DO INCIDENTE:

4.1. O incidente deverá ser devidamente documentado.

5. REVISÃO DOS PROCEDIMENTOS APLICADOS:

5.1. No caso de o incidente estar identificado no plano de Cibersegurança, deverá ser verificado se o procedimento implementado foi o previsto e se o mesmo surtiu o efeito desejado. Caso seja necessário, o incidente/ procedimento deverá ser acrescentado/ retificado no Plano de Cibersegurança.
5.2. Poderá ser necessário implementar outros serviços para reforço da segurança cibernética.

COMUNICAÇÃO DO INCIDENTE

A comunicação com os restantes elementos da equipa, ou com os elementos envolvidos no incidente, comunidade escolar, equipa Ciber.Edu e outras entidades, deverá ser efetuada pelo elemento 1 – responsável pela equipa de Cibersegurança da Escola ou Conselho Executivo.

06 | Política de segurança de informação da Escola

A criação de uma política de segurança da informação é um elemento estruturante da cibersegurança institucional. Enquanto instrumento estratégico, é essencial que esta política conte com a aprovação do Conselho Executivo e com o envolvimento e compromisso de toda a comunidade escolar. Ela constitui-se como o principal garante das boas práticas e um fator determinante na mitigação de riscos e na redução da exposição a ameaças no quotidiano escolar.

A sua efetivação concretiza-se através da definição e implementação de processos e procedimentos específicos, alinhados com os objetivos da instituição.

6.1 Introdução

A segurança da informação é fundamental para a proteção dos dados e sistemas da Escola. Esta política estabelece diretrizes para assegurar a confidencialidade, integridade e disponibilidade da informação, protegendo-a contra ameaças internas e externas, acidentais ou maliciosas.

6.2 Objetivos

- Proteger as informações da Escola contra acessos não autorizados.
- Garantir a integridade, exatidão e confiabilidade das informações.
- Assegurar a disponibilidade da informação para os utilizadores autorizados, sempre que necessário.
- Cumprir com os requisitos legais, regulamentares e normativos aplicáveis à proteção de dados e segurança da informação.

6.3 Âmbito de Aplicação

Esta política aplica-se a todos os membros da comunidade escolar, incluindo:

- Pessoal docente e não docente;
- Alunos;
- Prestadores de serviços;
- Visitantes e quaisquer outras partes que tenham acesso aos sistemas e informações da Escola.

6.4 Responsabilidades

- **Equipa de Cibersegurança:** Responsável pelo desenvolvimento, implementação, manutenção e monitorização das medidas de segurança da informação.
- **Conselho Executivo:** Deve apoiar e promover a política, garantindo os recursos necessários à sua execução.
- **Utilizadores da Rede Escolar:** Devem cumprir integralmente as diretrizes estabelecidas nesta política, adotando comportamentos seguros e reportando incidentes ou vulnerabilidades.

6.5 Diretrizes gerais

- **Confidencialidade**: A informação deve ser acessível apenas a pessoas autorizadas. Todos os utilizadores devem manter a confidencialidade dos dados pessoais e institucionais.
- **Integridade**: As informações devem ser precisas e completas. Qualquer alteração deve ser autorizada e com a possibilidade de ser rastreada.
- **Disponibilidade**: As informações e sistemas devem estar disponíveis para os utilizadores autorizados sempre que necessário.

6.6 Classificação da Informação

As informações da Escola devem ser classificadas conforme a sua sensibilidade e impacto em caso de comprometimento:

- **Pública**: Informações acessíveis à comunidade educativa. Normalmente publicadas no Web Site da Escola e a qual deve respeitar o estabelecido no presente Plano e legislação em vigor.
- **Pública no recinto escolar:** Informações afixadas na Escola, apenas acessíveis à comunidade escolar.
- **Interna**: Conjunto de informações que circulam entre os elementos da Escola, nomeadamente através de email, equipas no Teams, ou outros meios, e que obedecem a um conjunto de regras já estabelecidas na Escola.
- **Restrita**: Informações sensíveis acessíveis apenas a pessoas autorizadas.

6.7 Controlo de Acessos

- **Autenticação:** Uso de senhas fortes e quando possível, autenticação de dois fatores (2FA), para acesso aos sistemas informáticos da Escola.
- **Autorização:** Acesso concedido apenas aos elementos estritamente necessários.

6.8 Proteção contra ameaças

- **Antivírus e Antimalware**: Instalação e atualização regular de software de proteção.
- **Backup**: Realização de cópias de segurança periódicas das informações críticas.
- **Atualizações de Segurança**: Aplicação regular de *patches* e atualizações de segurança em todos os sistemas.

6.9 Resposta a Incidentes

A equipa de Cibersegurança da Escola deverá monitorizar regularmente os sistemas de informação, de forma a detetar incidentes e estar disponível para resolução dos incidentes relatados pelos membros da comunidade escolar.

No caso de incidente, será acionado o mapa de emergência Cibersegurança.

6.10 Sensibilização e Formação

A Escola promoverá a sensibilização da comunidade escolar sobre a importância da segurança da informação, através da realização de sessões formativas, criação de materiais, nomeadamente, panfletos/ *flyers*, que serão divulgados e publicados na página Web da Escola. Recomenda-se ainda, a utilização/ consulta dos recursos disponíveis em:

- Recursos para sensibilização do CNCS, disponível em: https://www.cncs.gov.pt/pt/recursos-para-sensibilizacao/
- Cursos e-learning do CNCS, disponível em: https://www.cncs.gov.pt/pt/cursos-e-learning/

6.11 Conformidade e Auditoria

A revisão e atualização desta política deverá ser efetuada, sempre que necessário, para garantir que se mantenha alinhada com as melhores práticas de segurança da informação e as necessidades da Escola.

A realização de auditorias pela equipa Ciber.EDU, poderá ser efetuada para verificar o cumprimento das diretrizes de segurança.

6.12 Consequências de não conformidade

O não cumprimento desta política poderá resultar na aplicação de medidas disciplinares ou restritivas, conforme previsto no Regulamento Interno da Escola, e/ou na legislação em vigor. Estas disposições aplicam-se a todos os membros da comunidade educativa: alunos, professores, pessoal não docente e visitantes.

07 | Procedimentos de notificação de incidentes

Para criar e implementar um conjunto de procedimentos de notificação de incidentes de cibersegurança que tenha impacto nas funções ou atividades críticas da Escola, é essencial definir claramente as responsabilidades e os fluxos de comunicação. A seguinte tabela especifica os tipos de incidentes, os níveis de gravidade, quem dentro da Escola deve ser informado, os procedimentos a serem realizados e ainda, alguns exemplos, de situações concretas que possam acontecer.

Tipo de incidente	Nível de incidente	Notificar	Procedimentos a adotar
Intrusão em Sistemas **Acesso não autorizado a sistemas de informação, frequentemente envolvendo a execução de código malicioso ou a exploração de vulnerabilidades. Esse tipo de incidente pode comprometer a integridade e confidencialidade das informações.**	Alto – Rede Administrativa	**Elemento 1** – Responsável pela equipa de Cibersegurança da escola e/ou (**Elementos 5 ou 6** – Polo da Fajã) e/ ou **Elemento 2** e/ ou **Elemento 3** (Técnicos de Sistemas de Informação e Comunicação)	1. Notificar imediatamente a equipa de cibersegurança (Elemento 1 e/ ou outros necessários à resolução) 2. Acionar plano de contenção e mitigação. 3. Realizar análise forense. 4. Implementar plano de recuperação. 5. Documentar o incidente e ações tomadas. 6. Realizar análise pós-incidente.
Exemplo: Um intruso ter acesso a um servidor da Escola e instalar *malware* para roubar dados			1. Detalhar o tipo de intrusão, a sua origem e qual o sistema/ equipamento em que foi detetado; 2. Isolar o sistema/ equipamento infetado de modo a evitar propagação, desconectando da rede em que se encontra afeto; 3. Detetar sinais de atividades anómalas ou comprometedoras, como alterações inesperadas no sistema/ equipamento, acesso não autorizado ou presença de *malware*; 4. Remover o *malware* e repor serviços e ou dados se necessário; 5. Registar os procedimentos realizados numa base de dados;

			6. Verificar se os procedimentos previstos foram respeitados e/ ou suficientes para resolução do incidente.
Fuga de Informação **Exposição não autorizada de informações sensíveis ou confidenciais. Pode resultar de ataques cibernéticos, erros humanos, ou falhas de segurança.**	Alto	**Elemento 1** – Responsável pela equipa de Cibersegurança da escola e/ou (**Elementos 5 ou 6** – Polo da Fajã) e/ ou **Elemento 2** e/ ou **Elemento 3** (Técnicos de Sistemas de Informação e Comunicação)	1. Notificar imediatamente a equipa de cibersegurança (Elemento 1 e/ ou outros necessários à resolução) 2. Informar partes afetadas; 3. Acionar plano de contenção e mitigação. 4. Realizar análise forense. 5. Realizar formação/ sensibilização junto das pessoas envolvidas; 6. Documentar o incidente e ações tomadas. 7. Realizar análise pós-incidente.
Exemplo: Dados pessoais de elementos da comunidade escolar a serem divulgados publicamente devido a um ataque *hacker*.			1. Detalhar o tipo de fuga de informação, nomeadamente que dados foram divulgados e os meios de divulgação; 2. Informar a(s) pessoa(s)/ entidade(s) afetada(s) de forma a ativar(em) outros procedimentos que possam ser necessários para evitar outros danos; 3. Na possibilidade de alterar/ retirar/ eliminar a informação divulgada, deverá ser efetuado com a maior brevidade possível; 4. Detetar sinais de atividades anómalas ou comprometedoras, como alterações inesperadas no sistema/ equipamento, acesso não autorizado ou presença de *malware*; 5. Sensibilizar a(s) pessoa(s) afetada(s) para o sucedido; 6. Registar os procedimentos realizados numa base de dados; 7. Verificar se os procedimentos previstos foram respeitados e/ ou suficientes para resolução do incidente.

Fraude **Atividades enganosas realizadas para obter ganho financeiro ou outras vantagens, frequentemente envolvendo roubo de identidade ou manipulação de transações.**	Alto – Rede Administrativa	**Elemento 1** – Responsável pela equipa de Cibersegurança da escola e/ou (**Elementos 5 ou 6** – Polo da Fajã) **Elemento 2** ou **Elemento 3** (Técnicos de Sistemas de Informação e Comunicação)	1. Notificar imediatamente a equipa de cibersegurança (Elemento 1 e/ ou outros necessários à resolução) 2. Informar partes afetadas; 3. Acionar plano de contenção e mitigação; 4. Realizar análise forense; 5. Implementar plano de recuperação; 6. Documentar o incidente e ações tomadas; 7. Realizar análise pós-incidente.
Exemplo: Um *hacker* a redirecionar pagamentos para uma conta fraudulenta.			1. Detalhar o tipo de acontecimento suspeito detetado; 2. Alterar credenciais de acesso ao sistema bancário envolvido; 3. Bloquear qualquer transação que tenha sido efetuada; 4. Informar a instituição bancária envolvida; 5. Detetar sinais de atividades anómalas ou comprometedoras, como alterações inesperadas no sistema/ equipamento, acesso não autorizado ou presença de *malware*; 6. Registar os procedimentos realizados numa base de dados; 7. Verificar se os procedimentos previstos foram respeitados e/ ou suficientes para resolução do incidente.
Roubo de Identidade **Obtenção e uso não autorizado de informações pessoais para realizar fraudes ou outras atividades ilegais.** **Comprometimento de Conta** **Acesso não autorizado a contas de utilizadores, geralmente obtido por meio de *phishing* ou exploração de vulnerabilidades.**	Médio	**Elemento 1** – Responsável pela equipa de Cibersegurança da escola e/ ou (**Elementos 5 ou 6** – Polo da Fajã) **Elemento 2** ou **Elemento 3**	1. Notificar imediatamente a equipa de cibersegurança (Elemento 1 e/ ou outros necessários à resolução) 2. Informar pessoa(s) afetada(s); 3. Acionar plano de contenção e mitigação; 4. Realizar análise forense; 5. Realizar formação/ sensibilização junto das pessoas envolvidas; 6. Documentar o incidente e ações tomadas; 7. Realizar análise pós-incidente.

PRR Plano de Recuperação e Resiliência · Região Autónoma da Madeira · República Portuguesa · Financiado pela União Europeia NextGenerationEU

Exemplo: Um atacante a usar informações pessoais roubadas para realizar ações em seu nome.		(Técnicos de Sistemas de Informação e Comunicação) **Elemento 4** (Coordenador TIC)	1. Detalhar o tipo de fuga de informação, nomeadamente que dados foram roubados; 2. Informar pessoa(s) afetada(s); 3. Alterar credenciais de acesso aos sistemas/ equipamentos a que a pessoa afetada tenha acesso ou que tenham sido roubados (da escola e/ ou pessoais); 4. Detetar sinais de atividades anómalas ou comprometedoras, como alterações inesperadas no sistema/ equipamento, acesso não autorizado ou presença de *malware*; 5. Sensibilizar a(s) pessoa(s) afetada(s) para o sucedido; 6. Registar os procedimentos realizados numa base de dados; 7. Verificar se os procedimentos previstos foram respeitados e/ ou suficientes para resolução do incidente.
Exemplo: Um *hacker* a obter acesso a contas de e-mail institucional (EDU) e enviar e-mails fraudulentos.			
Código Malicioso – *Malware* **Software destinado a causar danos ou comprometer a segurança de sistemas e redes, incluindo vírus, *worms*, *trojans*, entre outros.**	Médio	**Elemento 1** – Responsável pela equipa de Cibersegurança da escola e/ ou (**Elementos 5 ou 6** – Polo da Fajã) **Elemento 2** ou **Elemento 3** (Técnicos de Sistemas de Informação e Comunicação) **Elemento 4** (Coordenador TIC)	1. Notificar imediatamente a equipa de cibersegurança (Elemento 1 e/ ou outros necessários à resolução) 2. Acionar plano de contenção e mitigação; 3. Realizar análise forense; 4. Implementar plano de recuperação; 5. Realizar formação/ sensibilização junto da(s) pessoa(s) envolvida(s); 6. Documentar o incidente e ações tomadas; 7. Realizar análise pós-incidente.
Exemplo: Um *worm* que se propaga por uma rede, infetando múltiplos dispositivos.			1. Detalhar o tipo de intrusão, a sua origem e qual o equipamento e respetiva rede em que foi detetado; 2. Isolar o equipamento infetado de modo a evitar propagação, desconectando da rede em que se encontra afeto, bem como a respetiva rede; 3. Detetar sinais de atividades anómalas ou comprometedoras, como alterações inesperadas no

			equipamento e rede, acesso não autorizado ou presença de *worms ou outro malware*; 4. Remover o *malware* e repor o equipamento, ligação, serviço e dados se necessário; 5. Sensibilizar a(s) pessoa(s) afetada(s) para o sucedido; 6. Registar os procedimentos realizados numa base de dados; 7. Verificar se os procedimentos previstos foram respeitados e/ ou suficientes para resolução do incidente.
DDoS (Negação de Serviço Distribuído) **Ataque que sobrecarrega um serviço ou rede ou servidor com tráfego excessivo, tornando-o inacessível para utilizadores legítimos.**	Médio	**Elemento 1** – Responsável pela equipa de Cibersegurança da escola e/ ou (**Elementos 5 ou 6** – Polo da Fajã) **Elemento 2** ou **Elemento 3** (Técnicos de Sistemas de Informação e Comunicação) **Equipa Ciber.EDU**	1. Notificar imediatamente a equipa de cibersegurança (Elemento 1 e/ ou outros necessários à resolução); 2. Acionar plano de contenção e mitigação; 3. Realizar análise forense; 4. Documentar o incidente e ações tomadas; 5. Realizar análise pós-incidente.
Exemplo: Um site a ser bombardeado com solicitações de múltiplos dispositivos comprometidos, causando interrupção do serviço.			1. Detalhar o tipo de incidente, a sua origem e qual o serviço que está a sofrer o ataque; 2. Informar o fornecedor do serviço do que está a suceder; 3. Detetar sinais de atividades anómalas ou comprometedoras, como alterações inesperadas na rede (equipa Ciber.EDU); 4. Registar os procedimentos realizados numa base de dados; 5. Verificar se os procedimentos previstos foram respeitados e/ ou suficientes para resolução do incidente.
Ataque de *Ransomware* **Um tipo de *malware* que criptografa os dados da instituição e exige um resgate para restaurar o**	Alto	**Elemento 1** – Responsável pela equipa de	1. Notificar imediatamente a equipa de cibersegurança (Elemento 1 e/ ou outros necessários à resolução) 2. Informar autoridade(s); 3. Acionar plano de contenção e mitigação;

acesso. Os ataques de *ransomware* podem paralisar as operações até que os dados sejam recuperados.		Cibersegurança da escola e/ ou (**Elementos 5 ou 6** – Polo da Fajã) **Elemento 2** ou **Elemento 3** (Técnicos de Sistemas de Informação e Comunicação) **Equipa Ciber.EDU**	4. Realizar análise forense; 5. Implementar plano de recuperação; 6. Documentar o incidente e ações tomadas; 7. Realizar análise pós-incidente.
Exemplo: Um ataque em que todos os ficheiros da escola são criptografados e uma mensagem de resgate é exibida exigindo pagamento para a recuperação dos ficheiros.			1. Detalhar o tipo de intrusão, a sua origem e qual o equipamento e respetiva rede em que foi detetado; 2. Acionar autoridades competentes, incluindo a equipa Ciber.Edu; 3. Isolar o equipamento infetado de modo a evitar propagação, desconectando da rede em que se encontra afeto, bem como a respetiva rede; 4. Detetar sinais de atividades anómalas ou comprometedoras, como alterações inesperadas no equipamento e rede, acesso não autorizado ou presença de *malware* (com apoio da equipa Ciber.EDU e/ ou autoridades); 5. Remover o *malware* e repor o equipamento, ligação, serviço e dados se necessário (com apoio da equipa Ciber.EDU e/ ou autoridades); 6. Registar os procedimentos realizados numa base de dados; 7. Verificar se os procedimentos previstos foram respeitados e/ ou suficientes para resolução do incidente.

Engenharia Social **Manipulação de pessoas para realizar ações ou divulgar informações confidenciais. Pode incluir *phishing*, *pretexting*, *baiting*, entre outros.** ***Phishing*** **Tentativas fraudulentas de obter informações sensíveis disfarçando-se de uma entidade confiável em comunicações eletrónicas.**	Baixo	**Elemento 1** – Responsável pela equipa de Cibersegurança da escola e/ ou (**Elementos 5 ou 6** – Polo da Fajã) **Elemento 2** ou **Elemento 3** (Técnicos de Sistemas de Informação e Comunicação) **Elemento 4** (Coordenador TIC)	1. Notificar imediatamente a equipa de cibersegurança (Elemento 1 e/ ou outros necessários à resolução); 2. Acionar plano de contenção e mitigação; 3. Realizar análise forense; 4. Realizar formação/ sensibilização junto da(s) pessoa(s) envolvida(s); 5. Documentar o incidente e ações tomadas; 6. Realizar análise pós-incidente.
Exemplo: Um atacante a fingir ser funcionário de algum serviço prestado à escola e convencer um funcionário a fornecer a sua senha.			1. Detalhar a quem/ como e que acesso foi fornecido; 2. Revogar ou alterar imediatamente o acesso que foi cedido; 3. Averiguar se o sistema foi acedido e para que fins; 4. Sensibilizar a pessoa afetada para o sucedido; 5. Registar os procedimentos realizados numa base de dados; 6. Verificar se os procedimentos previstos foram respeitados e/ ou suficientes para resolução do incidente;
Exemplo: Um e-mail que parece ser de uma instituição bancária ou governamental a pedir que os funcionários redefinam as suas senhas num link falso.			

Tabela 3 – Procedimentos de notificação/ resolução de incidentes

Estes procedimentos de notificação de incidentes são essenciais para garantir uma resposta rápida e eficaz a qualquer ameaça de cibersegurança que possa ter impacto nas atividades críticas da organização. A colaboração e comunicação entre todos os elementos da Escola e equipa de Cibersegurança, são fundamentais para minimizar os danos e evitar futuras ocorrências.

08 | Inventariação de ativos

Listagem de equipamentos ativos na Rede Administrativa:

Em anexo B

Listagem de equipamentos ativos na Rede Escolar:

Em anexo C

Listagem de equipamentos ativos na Rede Manuais Digitais:

Em anexo D

09 | Mapas de rede

Principais mapas de Rede (mapas dos Bastidores). Para além dos aqui apresentados, foram efetuados todos os mapas de Rede:

Anexo E

10 | Recolha centralizada de registos (logs)

Os *logs* gerados pelo sistema operativo e pelas aplicações de suporte à atividade são cruciais para a análise e investigação de incidentes de cibersegurança. Estes fornecem um registo detalhado das atividades realizadas num sistema, permitindo identificar comportamentos anormais, detetar intrusões e determinar a causa de incidentes.

A Escola procede ao Backup dos *logs* dos equipamentos dos Serviços Administrativos semanalmente.

11 | Política de uso aceitável - PUA

Anexo F

12 | Manutenção de infraestruturas de cópias de segurança e reposição (Backup/Restore)

No mundo digital atual, a informação é um dos ativos mais valiosos e determinantes para o sucesso das organizações.

A perda de dados pode acarretar graves consequências, como a impossibilidade de realizar atividades essenciais para a Escola, resultando em perdas de dados, financeiras, prejuízos à reputação, exposição de informações confidenciais a terceiros. A falta de backups torna a escola mais vulnerável a *malwares* e *ransomwares* que podem criptografar dados e exigir pagamentos para recuperá-los.

Para garantir a segurança da informação e minimizar os riscos, é fundamental implementar soluções robustas de backup de dados. O backup consiste na criação de cópias de segurança dos dados num local diferente do original, permitindo a sua recuperação em caso de perda ou falha.

Na escolha de soluções de Backup é importante considerar alguns fatores como a dimensão/ complexidade da infraestrutura, volume e criticidade dos dados, procedimentos de recolha e de reposição e ainda, local físico de armazenamento.

É necessário ainda, testar e monitorizar o sistema de backup, através da realização de testes periódicos, de forma a garantir que no caso de necessidade, os dados serão restaurados com sucesso.

Ao nível dos **Serviços Administrativos**, onde se encontra a grande maioria os dados críticos da Escola, existe uma máquina local, onde todos os serviços e dados partilhados estão guardados e ao qual todos os equipamentos destes Serviços e Conselho Executivo, acedem no dia a dia. Existe uma segunda máquina, para realização de Backup diário. Este backup é efetuado de forma automatizada, normalmente programado para efetuar o backup no horário em que o funcionário está em hora de almoço ou após o horário de expediente. Semanalmente, é efetuado um segundo backup, para uma terceira máquina, encontrando-se esta num edifício (pavilhão) diferente dos anteriores. Ambos os servidores de backup, possuem discos em espelho, efetuando o backup do backup em cada máquina. Para finalizar, é efetuado semanalmente uma cópia de dados para disco externo. O acesso a estes servidores de backup é apenas efetuado pelos Técnicos de Sistemas de Tecnologias de Informação.

Outros dados da Escola, referentes a documentação interna de órgãos de gestão intermédia, são organizados/ armazenados em equipas do Teams e/ ou diretamente na *Cloud* do Serviço EDU.

13 | Proteção e gestão de equipamentos

A instalação de um antivírus e ou outros programas de proteção, são cruciais para garantir a segurança da informação e a proteção contra os diversos tipos de ameaças online.

O uso de um antivírus em todo o parque informático tem a vantagem dos dispositivos da rede estarem protegidos contra *malware*, vírus, *ransomware* e outras ameaças, reduzindo o risco de ataques cibernéticos, minimizando o impacto na rede e nos dados.

A Segurança dos equipamentos, não se restringe à utilização de um Software de antivírus, sendo importante implementar outras medidas.

Medidas essenciais para a proteção e gestão de equipamentos:

1. **Implementação de mecanismos de controlo de acesso** para restringir o uso de equipamentos apenas a utilizadores autorizados.
2. **Utilização de palavras-passe fortes e únicas** para cada conta, evitando a partilha de credenciais. Se possível, c**onsiderar o uso de autenticação multifator.**
3. Manter um bom **Sistema de Backup** atualizado e ativo.
4. **Promover a conscientização sobre segurança cibernética** através de panfletos/ *flyers*, sessões de sensibilização.
5. **Ensinar sobre os riscos online, as melhores práticas de segurança** e como utilizar os equipamentos de forma responsável.
6. **Prestar apoio técnico à comunidade** para auxiliar na resolução de problemas e dúvidas relacionadas à segurança dos dispositivos.
7. **Incentivar a comunicação aberta sobre incidentes de segurança** e a procura por ajuda em caso de dúvidas ou problemas.
8. **Sempre que se mostrar necessário, monitorar as atividades online dos utilizadores,** de modo a detetar comportamentos suspeitos e prevenir incidentes de segurança.
9. **Realizar manutenção preventiva de forma regular** nos equipamentos para garantir o seu bom funcionamento e identificar possíveis problemas.

10. **Implementar processos de gerenciamento de *patches* e vulnerabilidades** para identificar e corrigir falhas de segurança nos softwares e sistemas utilizados.
11. **Utilizar ferramentas de limpeza e atualização** para agilizar o processo e reduzir o risco de explorações.
12. **Implementar medidas de segurança física** para proteger os equipamentos contra roubo, perda ou danos. Manter os espaços onde existam equipamentos devidamente fechados.
13. **Manter um inventário atualizado dos equipamentos da Escola,** incluindo informações sobre modelo, número de série, software instalado e responsável pelo uso.
14. **Implementar um processo de descarte seguro de equipamentos eletrónicos** para garantir a proteção dos dados armazenados e evitar o acesso não autorizado a informações confidenciais.
15. **Utilizar métodos de destruição de dados confiáveis** e seguir as normas de proteção ambiental durante o processo de descarte.
16. **Atualizar com alguma regularidade o plano de resposta a incidentes** que define as ações a serem tomadas em caso de ataques cibernéticos, perda de dados ou outros problemas de segurança.
17. **Testar o plano de resposta a incidentes regularmente** para garantir sua efetividade.

Ao implementar estas medidas, a Escola estará mais protegida contra as diversas ameaças cibernéticas, contribuindo assim, para um ambiente seguro e confiável para a aprendizagem e o trabalho de toda a comunidade.

14 | Definição de planos de continuidade

O Plano de Continuidade é um elemento complementar importante à política de segurança interna.

Devem fazer parte deste plano os elementos essenciais que permitam à organização continuar em operação perante um qualquer desastre ou incidente que cause (ou tenha potencial para causar) uma disrupção significativa ou até total na atividade.

O plano de continuidade na área da cibersegurança será ativado em caso de:

- Interrupção prolongada da energia elétrica;
- Desastres naturais (inundações, incêndios, terremotos);
- Ameaças à segurança (violência, terrorismo);
- Pandemias ou surtos de doenças;
- Quebra de segurança de dados;
- Falhas nos sistemas de rede ou servidores críticos;
- Qualquer incidente que cause interrupção significativa nos sistemas informáticos da Escola.

14.1 Contactos de pessoas ou organizações:

Presidente do Conselho Executivo: José Bernardo Ferreira Gouveia

Telefone: 291 820 00 / Ext.: 14

Correio eletrónico: bernardogouveia@edu.madeira.gov.pt

Elemento 1 Responsável da equipa de Cibersegurança: José Carlos Santos Pestana

Telefone 291 820 00 / Ext.: 27

Correio eletrónico: carlospestana@edu.madeira.gov.pt

Elemento 2 da equipa Cibersegurança: Roberto Carlos Rocha Moniz

Correio eletrónico: roberto.rocha@edu.madeira.gov.pt

Elemento 3 da equipa Cibersegurança: Maria Luísa Alves Teles

Correio eletrónico: luisateles@edu.madeira.gov.pt

Elemento 4 da equipa Cibersegurança: Mariela Sousa da Silva

Correio eletrónico: marielasilva@edu.madeira.gov.pt

Elemento 5 da equipa Cibersegurança: Joaquim António Teixeira Rebelo

291 870 040 / Ext.: 222

Correio eletrónico: joaquim.rebelo@edu.madeira.gov.pt

Elemento 6 da equipa Cibersegurança: Hélder Rogério Carreira Vinagre

291 870 040 / Ext.: 229

Correio eletrónico: heldervinagre@edu.madeira.gov.pt

Equipa Ciber.EDU: Daniel Freitas | Email: ciberedu.dre@edu.madeira.gov.pt

- Polícia Judiciária: 291 220 800

- Polícia de Segurança Pública: 112

- Empresa de Eletricidade: 800 221 187

- Serviço de Telefone: MEO 800 206 000

14. 2 Papéis e responsabilidades na ativação:

- **Responsável da equipa de Cibersegurança:** Coordenar a resposta técnica, avaliar o impacto e iniciar a recuperação.
- **Presidente do CE:** Tomar decisões estratégicas, comunicar com as autoridades e comunidade escolar.
- **Equipa de Cibersegurança:** Garantir a continuidade dos sistemas informáticos e recuperação de dados.
- **Equipa Ciber.EDU:** Fornecer suporte e orientação na gestão do incidente.

14.3 Procedimentos a adotar na ativação:

1. Detetar o incidente e notificar imediatamente o responsável da equipa de Cibersegurança;
2. Entrar em contacto com a restante equipa de Cibersegurança, para avaliar o impacto do incidente e determinar a extensão da disrupção;
3. O responsável da equipa Cibersegurança deverá informar o presidente do CE e acionar a cadeia de contactos necessária;
4. A equipa Cibersegurança deverá desencadear um conjunto de procedimentos (ativação do plano de Continuidade) que se adaptem à situação em questão;
5. Todos os procedimentos devem ser devidamente documentados.

14. 4 Instalações alternativas:

Consoante a situação que desencadeou a ativação do Plano, poderá ser necessário alterar o espaço físico dos equipamentos com os serviços considerados críticos. Podendo ser uma sala de aula equipada com equipamentos móveis. No caso de ser necessário a evacuação total da Escola, poderão ser utilizadas as instalações (Polos) em zona geográfica distinta.

14. 5 Serviços alternativos:

A Escola está preparada para implementar ensino à distância, através do uso da Plataforma Teams. Outros meios de comunicação, nomeadamente o email, será também um recurso.

Alguns serviços realizados pelos Serviços Administrativos poderão ser temporariamente efetuados em papel e ou em localização remota.

15 | Definição de procedimentos de reação a incidentes

Esta ação pressupõe a identificação dos tipos de ataque mais comuns e os procedimentos necessários para mitigação ou resolução dos mesmos. A *tabela 3 - Procedimentos de notificação/ resolução de incidentes*, que se encontra no **ponto 7** deste Plano, lista um conjunto de incidentes para um conjunto de possíveis ataques passíveis de acontecer, e aos quais estão associados procedimentos a implementar/ seguir na mitigação e resolução dos mesmos.

Qualquer incidente de segurança cibernética deve ser comunicado a um membro da equipa de Cibersegurança, com preferência para o **elemento 1** – responsável pela equipa de Cibersegurança da Escola, que desencadeará os procedimentos necessários para resolução do incidente.

16 | Conhecimento das Políticas

A Escola está comprometida com a segurança digital de toda a comunidade educativa. Para garantir um ambiente escolar offline e online seguro e responsável, implementámos o Plano de Cibersegurança, que será divulgado:

1. **ao pessoal docente e não docente:**

   Através da realização de sessões formativas para explicar as medidas do Plano, boas práticas digitais e procedimentos de segurança. Estas sessões visam capacitar todos os colaboradores para prevenir riscos e proteger dados.

2. **aos alunos:**

   Os alunos serão informados pelo titular/ diretor de turma sobre a existência e importância da Política de Cibersegurança, promovendo comportamentos seguros na utilização das tecnologias.

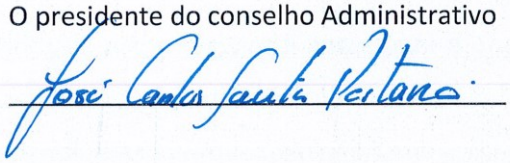
3. **aos pais e encarregados de educação:**

A Escola comunicará o Plano de Cibersegurança através de boletins informativos e nas reuniões regulares com os titulares/ diretores de turma, garantindo que todos conhecem as medidas, de forma a apoiar os seus educandos.

Conselho Administrativo

Parecer favorável em reunião de 9 de dezembro de 2025

O presidente do conselho Administrativo



Conselho Executivo

Aprovado por unanimidade em reunião de 9 de dezembro de 2025

O Presidente do Conselho Executivo