Região Autónoma da Madeira
Governo Regional

Secretaria Regional
de Educação, Ciência e Tecnologia
Direção Regional de Educação

Plano de Cibersegurança da Escola EB/PE de Santo António e Curral das Freiras

Ciber.EDU

2026 Abril

PRR Plano de Recuperação e Resiliência

REGIÃO AUTÓNOMA DA MADEIRA

REPÚBLICA PORTUGUESA

Financiado pela União Europeia
NextGenerationEU

Índice

Índice de tabelas

1. Introdução

A transformação digital das escolas trouxe novas oportunidades de aprendizagem, colaboração e gestão, mas também novos riscos. Num contexto em que alunos, docentes e funcionários utilizam diariamente dispositivos, plataformas online e redes internas, a cibersegurança tornou-se um pilar essencial para garantir a continuidade pedagógica, a proteção de dados pessoais e o bom funcionamento das infraestruturas tecnológicas. A escola, enquanto espaço educativo e formativo, tem a responsabilidade de assegurar que todos os utilizadores dispõem de um ambiente digital seguro, confiável e resiliente.

Este Plano de Cibersegurança estabelece a visão, as responsabilidades e os procedimentos necessários para prevenir incidentes, responder eficazmente a ameaças e promover uma cultura de segurança digital em toda a comunidade escolar. A sua implementação é fundamental para proteger informação sensível, garantir a integridade dos sistemas, minimizar interrupções e cumprir as obrigações legais e regulamentares aplicáveis.

Ao longo deste documento são apresentados os elementos estruturantes da estratégia de cibersegurança da escola, incluindo:

- **Constituição da Equipa de Cibersegurança**, responsável pela coordenação das ações e pela resposta a incidentes.
- **Identificação de funções e atividades críticas**, essenciais para o funcionamento diário da escola.
- **Cadeia de responsabilidade**, definindo quem decide, quem executa e quem comunica em cada situação.
- **Mapa de emergência de cibersegurança**, com procedimentos imediatos em caso de incidente.
- **Política de Segurança da Informação**, que orienta o uso responsável dos sistemas e dados.
- **Procedimentos de notificação de incidentes**, garantindo rapidez e clareza na comunicação interna e externa.
- **Inventariação de ativos e mapas de rede**, fundamentais para conhecer e proteger a infraestrutura tecnológica.
- **Recolha centralizada de registos (logs)**, permitindo monitorização e deteção precoce de anomalias.

- **Política de Uso Aceitável (PUA)**, que define regras para alunos, docentes e funcionários.
- **Estratégias de backup e recuperação**, assegurando a continuidade dos serviços em caso de falha.
- **Proteção e gestão de equipamentos**, incluindo dispositivos da escola e equipamentos pessoais autorizados.
- **Planos de continuidade e procedimentos de reação a incidentes**, garantindo resiliência operacional.
- **Promoção do conhecimento das políticas**, reforçando a literacia digital e a responsabilidade de todos.

Este plano pretende ser um instrumento prático, atualizado e adaptável, que apoia a nossa escola, Escola B/PE de Santo António e Curral das freiras, na construção de um ambiente digital seguro e preparado para os desafios atuais e futuros.

2. Responsável da Equipa de Cibersegurança

O responsável de segurança é o ponto de contato da organização do ponto de vista técnico/operacional e deverá ser capaz de responder às solicitações da equipa CiberEDU sendo esperada disponibilidade para contactos de emergência fora do horário de expediente. Este deverá conhecer bem a organização a nível de gestão, quer do ponto de vista técnico, devendo ser capaz de reencaminhar internamente as solicitações do CiberEDU.

Elemento	Cargo
1	Equipa responsável por apoiar as escolas e os serviços da DRE na área de Cibersegurança
2	Vice-presidente do Conselho Executivo; Responsável da equipa de Cibersegurança
3	Coordenador TIC
4	Coordenadora 1.º Ciclo
5	Técnico de Informática
6	Professor de Informática
7	Professora de Informática

Tabela 1: Equipa de Cibersegurança

3. Identificação de funções ou atividades críticas

A identificação de funções e atividades críticas constitui um dos pilares fundamentais da estratégia de cibersegurança da escola. Num ambiente educativo cada vez mais dependente de sistemas digitais - desde plataformas de aprendizagem até sistemas administrativos, redes internas e equipamentos utilizados por alunos e docentes - é essencial compreender quais são os processos cuja interrupção teria impacto significativo no funcionamento diário da instituição.

Este levantamento permite reconhecer os serviços, recursos e operações que garantem a continuidade pedagógica, administrativa e operacional da escola. Ao identificar estas funções críticas, torna-se possível priorizar medidas de proteção, definir níveis adequados de segurança, planear respostas a incidentes e assegurar que, mesmo perante falhas tecnológicas ou ataques informáticos, a escola mantém a sua capacidade de ensinar, comunicar e operar de forma segura.

Aqui serão descritas as atividades essenciais ao funcionamento da escola, os sistemas que as suportam e os riscos associados à sua indisponibilidade, servindo de base para a definição de estratégias de mitigação, continuidade e recuperação.

Serviço / Aplicação	Rede	Nível de prioridade	Dependências	Impacto	Alternativa
Servidor Windows com partilha de ficheiros	Administrativa	Alta	Secretaria utiliza para consulta de modelos de documentos e para guardar documentos digitalizados	Alto	Modelos arquivados em dossier
Servidor tab	Administrativa	Alta	Pagamentos efetuados na escola	Alto	Registo em papel e pagamento em dinheiro
Servidor de Domínio	Administrativa	Médio	Autenticação e acesso aos dispositivos de rede	Médio	Autenticação local
Servidor de Domínio	Escolar	Médio	Autenticação e acesso aos dispositivos de rede	Médio	Autenticação local

Tabela 2: Funções ou atividades críticas

4. Cadeia de Responsabilidade

A **Cadeia de Responsabilidade** define, de forma clara e hierárquica, quem responde por cada decisão, ação e comunicação relacionada com a cibersegurança da escola. O objetivo é garantir que todos os intervenientes sabem exatamente o seu papel, evitando ambiguidades durante a operação normal e, sobretudo, em situações de incidente.

A cadeia de responsabilidade assegura:

- Clareza na tomada de decisão;
- Rapidez na resposta a incidentes;
- Responsabilização individual e coletiva;
- Coerência na aplicação das políticas de segurança;
- Comunicação eficaz entre equipas, Conselho Executivo e entidades externas.

a) Estrutura da Cadeia de Responsabilidade

1. **Equipa Ciber.Edu:** estrutura de apoio criada no âmbito da Direção de Serviços de Tecnologias e Ambientes Inovadores de Aprendizagem (DSTEIA)**,** integrada na Divisão de Tecnologias, Segurança e Infraestruturas. O seu propósito é reforçar a cibersegurança nas escolas e apoiar diretamente as equipas locais responsáveis pela proteção digital.
2. **Conselho Executivo da Escola:** responsável máxima pela aprovação das políticas de segurança, pela disponibilização de recursos e pela validação das ações estratégicas. O Conselho Executivo é a entidade que assume a responsabilidade institucional perante autoridades externas.
3. **Coordenador de Cibersegurança:** figura central na gestão da segurança da informação. Supervisiona a implementação das políticas, coordena a Equipa de Cibersegurança e garante a articulação com a Conselho Executivo. É o ponto de contacto principal em caso de incidentes.
4. **Equipa de Cibersegurança:** grupo responsável pela monitorização contínua, gestão de vulnerabilidades, inventário de ativos, análise de logs, manutenção de backups e execução dos planos de resposta a incidentes. Atua de acordo com as orientações do Coordenador.
5. **Responsáveis de TIC / Administradores de Sistemas:** executam tarefas técnicas específicas, como gestão de redes, controlo de acessos, manutenção de equipamentos e implementação de medidas de proteção. São responsáveis por reportar anomalias e incidentes à Equipa de Cibersegurança.

6. **Docentes e Funcionários:** responsáveis por cumprir a Política de Uso Aceitável (PUA), reportar comportamentos suspeitos, proteger credenciais e garantir o uso seguro dos equipamentos e plataformas digitais da escola.
7. **Alunos:** devem seguir as regras definidas na PUA, utilizar os recursos tecnológicos de forma responsável e comunicar qualquer situação anómala aos docentes ou funcionários.
8. **Entidades Externas (fornecedores, técnicos, parceiros):** devem cumprir as normas de segurança definidas pela escola e atuar apenas mediante autorização do Conselho Executivo ou do Coordenador de Cibersegurança.

b) Fluxo de Comunicação e Escalonamento

- **Incidentes menores** (ex.: falha de acesso, suspeita de phishing) → Reportados ao docente/funcionário → Equipa de Cibersegurança.
- **Incidentes moderados** (ex.: falha de serviço, anomalias de rede) → Equipa de Cibersegurança → Coordenador → Conselho Executivo.
- **Incidentes críticos** (ex.: ransomware, fuga de dados, intrusão) → Coordenador → Conselho Executivo → Entidades externas competentes (ANACOM, CNCS, Polícia Judiciária, etc., conforme aplicável).

A Equipa de Cibersegurança da Escola de Santo António e Curral das Freiras foi nomeada e apresentada no primeiro Conselho Pedagógico, no ano letivo de 2025/2026. Foi ainda publicitado no site da escola essa informação no endereço: https://escoladigital.madeira.gov.pt/ebsantonio/ciberseguranca

5. Política de Segurança de Informação (PSI) da Escola

A Política de Segurança da Informação de uma Escola é o documento que define as regras, responsabilidades e práticas necessárias para proteger os dados, os sistemas e os recursos tecnológicos da instituição. Estabelece como a informação deve ser utilizada, armazenada, partilhada e protegida por todos os membros da comunidade escolar - alunos, docentes, funcionários, Conselho Executivo e parceiros externos.

A sua importância reside no facto de garantir a confidencialidade, integridade e disponibilidade da informação, prevenindo acessos indevidos, perdas de dados, ataques informáticos e utilizações incorretas dos sistemas. Além disso, assegura o cumprimento de obrigações legais, como o RGPD, e promove uma cultura de responsabilidade digital em toda a escola.

Esta política aplica-se a:

- Todos os utilizadores dos sistemas da escola (alunos, docentes, assistentes operacionais, assistentes técnicos, Conselho Executivo e entidades externas autorizadas).
- Todos os equipamentos, redes, plataformas digitais, serviços cloud e dados geridos pela escola.
- Todas as atividades que envolvam criação, armazenamento, transmissão ou eliminação de informação.

a) Princípios de Segurança

- Confidencialidade: A informação só pode ser acedida por pessoas autorizadas.
- Integridade: Os dados devem ser exatos, completos e protegidos contra alterações indevidas.
- Disponibilidade: Os sistemas e dados devem estar acessíveis quando necessários para fins pedagógicos e administrativos.
- Legalidade: Cumprimento do RGPD e demais legislação aplicável.
- Responsabilidade: Cada utilizador é responsável pelo uso adequado dos recursos digitais.

b) Regras Gerais de Utilização

- Utilização obrigatória de credenciais individuais e intransmissíveis.
- Proibição de instalação de software não autorizado.
- Acesso à rede Wi-Fi apenas através de perfis definidos.
- Utilização responsável de e-mail institucional e plataformas educativas.
- Proibição de armazenamento de dados pessoais em dispositivos não protegidos.
- Obrigatoriedade de atualização regular de software e antivírus.

c) Gestão de Acessos

- Perfis de acesso definidos conforme função (aluno, docente, funcionário, Conselho Executivo).
- Acesso a dados sensíveis limitado a pessoal autorizado.
- Desativação de contas de utilizadores que deixem a escola.
- Revisão periódica dos privilégios de acesso.

d) Proteção de Dados Pessoais

- Tratamento de dados apenas para finalidades educativas e administrativas.
- Minimização de dados recolhidos.
- Armazenamento seguro e eliminação adequada após o período legal.
- Comunicação de dados a terceiros apenas mediante autorização e necessidade.

e) Segurança dos Equipamentos

- Equipamentos devem ser mantidos atualizados e protegidos por antivírus.
- Dispositivos móveis devem ter bloqueio por PIN ou palavra-passe.
- Proibição de utilização de dispositivos pessoais para dados sensíveis sem autorização.
- Reporte imediato de perda, roubo ou dano.

f) Segurança da Rede e Infraestruturas

- Monitorização contínua da rede.
- Segmentação entre redes administrativas, docentes e de alunos.
- Implementação de firewalls, filtragem de conteúdos e proteção contra intrusões.
- Backups regulares e testados.

g) Formação e Sensibilização

- Sessões anuais de formação para docentes e funcionários (cursos disponíveis em https://www.cncs.gov.pt/pt/cursos-e-learning/).
- Atividades de literacia digital e segurança para alunos.
- Divulgação contínua de boas práticas (materiais disponíveis em https://www.cncs.gov.pt/pt/recursos-para- sensibilizacao/).

h) Resposta a Incidentes

- Existência de uma Equipa de Cibersegurança escolar.
- Procedimentos definidos para deteção, análise, contenção e recuperação.
- Comunicação obrigatória de incidentes ao Conselho Executivo e, quando necessário, a entidades externas.

i) Revisão da Política

A PSI deve ser revista anualmente ou sempre que ocorrerem alterações tecnológicas, legais ou organizacionais relevantes.

6. Procedimentos de Notificação de Incidentes de Cibersegurança

1.º O que é considerado incidente

Qualquer evento que comprometa ou possa comprometer:

- Dados pessoais;
- Funcionamento dos sistemas;
- Integridade da rede;
- Equipamentos ou contas de utilizador.

Exemplos: phishing, malware, perda de equipamento, acesso indevido, falha de serviço, fuga de dados.

2.º Quem deve reportar

Todos os utilizadores da escola: alunos, docentes, funcionários e parceiros externos.

3.º Como reportar

O incidente deve ser comunicado imediatamente através de um dos seguintes canais definidos pela escola:

- Formulário interno de incidentes;
- Comunicação direta ao docente ou funcionário, no caso de alunos;
- Contacto telefónico com o Conselho Executivo (em incidentes críticos).

4.º Informação mínima a incluir

- Descrição do incidente;
- Data e hora;
- Equipamento ou conta afetada;
- Ações já realizadas (se existirem);
- Evidências disponíveis (capturas de ecrã, mensagens, etc.).

5.º Fluxo de Escalonamento

1. **Utilizador** → comunica à **Equipa de Ciber.Edu ou Equipa de Cibersegurança**;
2. **Equipa** → avalia gravidade;
3. Se necessário: **Coordenador de Cibersegurança** → **Conselho Executivo**;
4. Em incidentes graves: **Conselho Executivo** → **Entidades externas** (CNCS, PJ, ANACOM, etc.).

6. Ações após o reporte

- Registo do incidente;
- Análise técnica;
- Contenção e mitigação;
- Recuperação e reposição de serviços;
- Comunicação interna e externa (se aplicável);
- Relatório final e lições aprendidas.

Descrição do Incidente	Nível do Incidente	Elementos	Procedimentos a adotar
Phishing / Tentativa de fraude	Baixo a Médio	Docente/Funcionário; Equipa de Cibersegurança	- Não clicar em links nem abrir anexos; - Enviar captura de ecrã ou e-mail suspeito; - Equipa analisa e bloqueia remetente; - Sensibilização dos utilizadores afetados.
Malware / Vírus detetado	Médio	Equipa de Cibersegurança; Coordenador TIC	- Isolar o equipamento da rede; - Não tentar remover manualmente; - Equipa executa análise e limpeza; - Verificar backups e restaurar se necessário.
Acesso indevido a contas ou sistemas	Médio a Alto	Equipa de Cibersegurança; Conselho Executivo	- Alterar palavra-passe imediatamente; - Identificar utilizador e origem do acesso; - Rever permissões e registos (logs); - Notificar encarregados de educação se envolver alunos.

Perda ou roubo de equipamento	Médio	Conselho Executivo; Equipa de Cibersegurança	- Identificar dados armazenados no dispositivo; - Bloquear contas associadas; - Ativar localização ou limpeza remota (se possível); - Registar ocorrência e avaliar impacto.
Falha de serviço crítico (Wi-Fi, plataformas, servidores)	Médio	Equipa de Cibersegurança; Coordenador TIC	- Registar hora e impacto; - Verificar origem (falha técnica, sobrecarga, ataque); - Implementar medidas de mitigação; - Comunicar previsão de resolução.
Fuga de dados / Violação de dados pessoais	Alto	Conselho Executivo; Encarregado de Proteção de Dados; Entidades externas (se necessário)	- Identificar dados expostos e utilizadores afetados; - Conter a origem da fuga; - Avaliar risco para titulares dos dados; - Notificar CNPD se aplicável; - Comunicar às famílias quando necessário.
Ataque à rede (DDoS, intrusão, ransomware)	Crítico	Conselho Executivo; Equipa de Cibersegurança; Entidades externas (CNCS, PJ)	- Desligar sistemas afetados; - Isolar segmentos da rede; - Não pagar resgates nem negociar; - Ativar plano de continuidade; - Recolher evidências para investigação.
Comportamento digital abusivo (cyberbullying, uso indevido)	Baixo a Médio	Docente; Conselho Executivo; Psicologia/Serviços Educativos	- Recolher evidências (capturas, mensagens); - Avaliar gravidade e impacto; - Aplicar medidas disciplinares conforme regulamento; - Acompanhar alunos envolvidos.
Instalação de software não autorizado	Baixo	Docente/Funcionário; Equipa de Cibersegurança	- Remover software; - Verificar integridade do sistema; - Reforçar regras da PUA; - Registar ocorrência.

Tentativa de acesso físico não autorizado a equipamentos	Médio	Conselho Executivo; Equipa de Cibersegurança	- Verificar danos ou acessos; - Rever câmaras e registos; - Reforçar controlo de acessos; - Registar incidente.

Tabela 3: Procedimentos de Reação a Incidentes

7. Inventariação de ativos

A inventariação de ativos é essencial para identificar todos os recursos tecnológicos e informacionais que precisam de proteção. Permite conhecer o que existe, onde está, quem utiliza e qual o grau de risco de cada elemento. Este inventário deve ser atualizado regularmente pela Equipa de Cibersegurança e pelos responsáveis TIC.

Categoria	Ativo	Descrição / Função	Localização	Responsável	Grau de risco	Observações
Infraestrutura de Rede	Router principal	Acesso à internet e gestão de tráfego	Sala TIC / Quadro elétrico	Administrador TIC	Alta	Configuração protegida
	Switches	Distribuição de rede interna	Diversas salas técnicas	Administrador TIC	Alta	Segmentação por VLAN
	Firewall	Proteção perimetral	Sala TIC	Administrador TIC	Alta	Regras atualizadas
Servidores	Servidor de ficheiros	Armazenamento de documentos internos	Sala TIC	Administrador TIC	Alta	Backups diários
	Servidor de autenticação	Gestão de contas e acessos	Sala TIC	Administrador TIC	Alta	Acesso restrito
	Servidor de plataformas educativas	Acesso a Moodle/Teams /Outros	Cloud / Local	Conselho Executivo + TIC	Média	Depende do fornecedor
Equipamentos Informáticos	Computadores de secretária	Uso administrativo e pedagógico	Salas, biblioteca, secretaria	Docentes/Funcionários	Média	Atualizações automáticas

	Portáteis	Uso docente e administrativo	Diversos	Docentes/Funcionários	Média	Política de uso aplicável
	Tablets	Uso pedagógico	Salas de aula	Docentes	Baixa a Média	Gestão MDM recomendada
	Projetores / Quadros interativos	Apoio ao ensino	Salas de aula	Docentes	Baixa	Manutenção periódica
Dispositivos Móveis	Telemóveis institucionais	Comunicação interna	Conselho Executivo / Funcionários	Conselho Executivo	Média	Proteção por PIN
Sistemas e Software	Sistema de gestão escolar	Gestão administrativa e pedagógica	Secretaria / Conselho Executivo	Conselho Executivo	Alta	Dados sensíveis
	Antivírus	Proteção de endpoints	Todos os equipamentos	TIC	Alta	Atualização automática
	Sistema de backups	Cópias de segurança	Servidor / Cloud	TIC	Alta	Testes mensais
Dados e Informação	Dados pessoais de alunos	Identificação, avaliações, processos	Secretaria / Cloud	Conselho Executivo	Alta	Proteção RGPD
	Dados de funcionários	Processos administrativos	Secretaria	Conselho Executivo	Alta	Acesso restrito
	Documentos pedagógicos	Planificações, materiais	Cloud / Equipamentos	Docentes	Média	Backup automático
Serviços Externos	Plataforma de e-mail	Comunicação institucional	Cloud	Conselho Executivo + TIC	Alta	MFA recomendado
	Plataforma de gestão de refeições	Gestão de pagamentos	Cloud	Secretaria	Média	Dados financeiros
	Plataforma de vigilância	Segurança física	Sala técnica	Conselho Executivo	Alta	Acesso restrito

Tabela 4: Inventário de Ativos

8. Mapas de rede

O mapa de rede descreve a estrutura lógica e física da infraestrutura tecnológica da escola, identificando os principais equipamentos, ligações e segmentações de rede. Esta visão permite compreender como circula a informação, onde existem pontos críticos e como se distribuem os acessos.

9. Recolha centralizada de registos (logs)

A Recolha Centralizada de Registos (logs) é uma das peças mais importantes de um Plano de Cibersegurança escolar. É através dos logs que a escola consegue detetar comportamentos anómalos, investigar incidentes e garantir conformidade com políticas internas e legislação.

A recolha centralizada de registos consiste na agregação, num único ponto, de todos os logs gerados pelos diversos sistemas da escola - servidores, computadores, firewall, rede Wi-Fi, plataformas digitais e aplicações administrativas. Em vez de cada equipamento guardar os seus próprios registos de forma isolada, estes são enviados para um sistema central, facilitando a monitorização, análise e resposta a incidentes.

a) Tipos de Registos a Recolher

- **Autenticação e acessos** (entradas e saídas de utilizadores);
- **Eventos de rede** (ligações, bloqueios, tráfego suspeito);
- **Eventos de firewall** (tentativas de intrusão, portas bloqueadas);
- **Registos de antivírus** (deteção de malware, quarentena);
- **Logs de servidores** (ficheiros, permissões, falhas de serviço);
- **Atividade de plataformas educativas e administrativas**;
- **Eventos de dispositivos finais** (computadores, tablets, impressoras de rede).

b) Boas Práticas de Implementação

- Utilizar um **servidor central de logs** (local ou cloud).
- Definir **retenção mínima** (ex.: 6 a 12 meses).
- Garantir que os logs são protegidos contra alterações.
- Implementar alertas automáticos para eventos críticos.
- Restringir o acesso aos logs apenas à Equipa de Cibersegurança.
- Realizar revisões periódicas para identificar padrões ou vulnerabilidades.

Tipo de Registo	Descrição	Periodicidade de Recolha	Local de Armazenamento
Logs de Autenticação	Entradas e saídas de utilizadores, falhas de login, alterações de permissões	Recolha contínua (tempo real)	Servidor central de logs / Cloud segura
Logs da Firewall	Tentativas de intrusão, tráfego bloqueado, regras aplicadas	Recolha contínua	Servidor de logs / Appliance da firewall
Logs de Rede	Ligações, desconexões, alterações de portas, eventos anómalos	Recolha diária	Servidor central de logs
Logs de Antivírus / Endpoint Protection	Deteção de malware, quarentena, atualizações	Recolha diária ou em tempo real	Consola de gestão do antivírus
Logs de Servidores	Acessos a ficheiros, erros de sistema, alterações de configuração	Recolha diária	Servidor de logs / Diretório seguro
Logs de Plataformas Educativas	Acessos, submissões, alterações de contas, erros	Recolha automática conforme fornecedor	Cloud do fornecedor / Exportação periódica
Logs de Sistemas Administrativos	Acessos, alterações de dados, operações críticas	Recolha diária	Servidor administrativo / Cloud
Logs de Impressoras de Rede	Utilização, acessos, falhas	Recolha semanal	Servidor de impressão
Logs de Videovigilância (CCTV)	Acessos ao sistema, falhas, alertas	Recolha diária	Sistema de CCTV / NAS seguro
Logs de Backups	Sucesso/falha de cópias de segurança, alertas	Recolha diária	Servidor de backup / Cloud
Logs de Dispositivos Finais	Erros, atualizações, eventos críticos	Recolha semanal ou automática via agente	Servidor de gestão de dispositivos

Tabela 5: Tipos de registos, padrões e vulnerabilidades

10. Política de uso aceitável (PUA)

A Política de Uso Aceitável (PUA), é um conjunto de regras estabelecidas por uma organização para garantir a segurança, integridade e o uso ético dos seus sistemas informáticos, redes e equipamentos. Este documento define o que é permitido e proibido, visando proteger a infraestrutura e prevenir abusos, geralmente aplicável a funcionários, alunos ou docentes.

11. Manutenção de infraestruturas de cópias de segurança e reposição (Backup/Restore)

A manutenção das infraestruturas de cópias de segurança e reposição (Backup/Restore) consiste num conjunto de procedimentos contínuos que garantem que todos os dados essenciais da escola permanecem protegidos e podem ser recuperados sempre que necessário. Este processo envolve não apenas a criação regular de cópias de segurança, mas também a verificação da sua integridade, a proteção dos locais onde são armazenadas e a realização periódica de testes de reposição para assegurar que os sistemas podem ser restaurados sem perda significativa de informação.

As cópias de segurança abrangem todos os dados críticos da escola, incluindo documentos administrativos, bases de dados de plataformas educativas, configurações de servidores e equipamentos de rede, registos de logs e, sempre que aplicável, imagens completas dos sistemas. Estas cópias são realizadas de forma automática através de um servidor de backups e de um NAS seguro, complementadas por um repositório externo na cloud que garante redundância geográfica. A política de backup define que são efetuadas cópias incrementais diárias, cópias completas semanais e mensais, bem como backups extraordinários sempre que ocorrem alterações significativas na infraestrutura ou nos sistemas.

Os backups são armazenados em locais distintos. Garantindo assim, que apenas pessoas autorizadas podem consultar ou restaurar dados. A encriptação é obrigatória tanto durante o armazenamento como durante a transferência dos dados, e todos os ficheiros são sujeitos a verificações automáticas de integridade para detetar eventuais corrupções. Os registos das operações de backup são enviados para o sistema centralizado de logs, permitindo auditoria e rastreabilidade.

A manutenção regular destas infraestruturas inclui a verificação do sucesso das cópias de segurança, a análise de alertas e falhas, e a confirmação de que existe espaço suficiente nos sistemas de armazenamento. É realizado periodicamente, um teste de reposição parcial, que consiste na recuperação de ficheiros individuais para garantir que os backups estão funcionais. Além disso, o software de backup é atualizado regularmente para garantir compatibilidade e segurança.

O processo de reposição (restore) segue uma sequência rigorosa. O incidente é identificado, seleciona-se o backup mais recente e íntegro, valida-se a autorização do Conselho Executivo e procede-se à recuperação no ambiente adequado, seja parcial ou total. Após a reposição, o sistema é testado para confirmar o seu funcionamento normal e o processo é registado, sendo posteriormente comunicada a resolução aos utilizadores envolvidos. Em situações que envolvam dados pessoais, o Encarregado de Proteção de Dados acompanha o processo para garantir conformidade com o RGPD.

A eficácia deste sistema é avaliada através de indicadores como a taxa de sucesso dos backups, a regularidade dos testes de reposição e a inexistência de perdas permanentes de dados. A manutenção adequada das infraestruturas de backup e restore é essencial para garantir a continuidade das operações da escola, proteger a informação sensível e assegurar uma resposta rápida e eficaz perante qualquer incidente que comprometa a integridade ou disponibilidade dos dados.

12. Proteção e gestão de equipamentos

A proteção e a gestão de equipamento constituem um elemento essencial da segurança da informação numa escola, garantindo que todos os dispositivos utilizados pela comunidade educativa são mantidos em condições adequadas, configurados de forma segura e protegidos contra acessos indevidos ou utilização inadequada. Esta gestão abrange computadores de secretária, portáteis, tablets, impressoras de rede, quadros interativos, equipamentos de rede e quaisquer outros dispositivos que se liguem à infraestrutura digital da escola. O objetivo principal é assegurar que cada equipamento funciona de forma fiável, está atualizado e cumpre as políticas internas de segurança.
Todos os equipamentos devem ser inventariados e associados a um responsável direto, garantindo que existe controlo sobre quem utiliza cada dispositivo e em que condições. A configuração inicial de qualquer equipamento deve incluir a instalação de software autorizado, antivírus atualizado, políticas de palavra-passe, encriptação quando aplicável e ligação às redes adequadas, respeitando a segmentação por VLANs. A utilização de contas partilhadas deve ser evitada, privilegiando sempre credenciais individuais para permitir rastreabilidade e responsabilização.

A manutenção regular dos equipamentos é fundamental para prevenir falhas e vulnerabilidades. Esta manutenção inclui a instalação de atualizações de segurança, a

verificação do estado físico dos dispositivos, a limpeza de software desnecessário e a monitorização de eventuais comportamentos anómalos. Os equipamentos que acedem a dados sensíveis, como os utilizados pelo Conselho Executivo ou secretaria, devem ter medidas adicionais de proteção, incluindo encriptação de disco, bloqueio automático de sessão e restrições de acesso físico. Em caso de avaria, perda ou roubo, o incidente deve ser comunicado de imediato ao Conselho Executivo, permitindo a ativação dos procedimentos de resposta e, quando necessário, a atuação do Encarregado de Proteção de Dados.

A gestão de equipamento inclui também o controlo de acessos físicos. Os dispositivos mais sensíveis devem ser guardados em locais seguros, como armários fechados ou salas com acesso restrito. Os equipamentos móveis, como portáteis e tablets, devem ser transportados e utilizados de forma responsável, garantindo que não são deixados sem vigilância em espaços públicos ou acessíveis a terceiros. Sempre que possível, deve ser ativada a funcionalidade de localização e bloqueio remoto, permitindo proteger a informação em caso de extravio.

A reposição e substituição de equipamentos deve seguir critérios de segurança, garantindo que dispositivos antigos são corretamente apagados antes de serem descartados ou reutilizados. A eliminação segura de dados é obrigatória, evitando que informação sensível possa ser recuperada por terceiros. Da mesma forma, a aquisição de novos equipamentos deve considerar requisitos mínimos de segurança, compatibilidade com as políticas internas e capacidade de integração com os sistemas de gestão existentes.

A proteção e gestão de equipamento contribuem diretamente para a resiliência digital da escola, reduzindo o risco de incidentes, garantindo a continuidade das atividades e protegendo a privacidade de alunos, docentes e funcionários. Uma abordagem consistente e rigorosa permite assegurar que todos os dispositivos funcionam de forma segura e eficiente, reforçando a confiança na infraestrutura tecnológica da instituição.

13. Definição de planos de continuidade

A definição do plano de continuidade deve estabelecer de forma clara as condições em que é ativado, os responsáveis pela sua execução e os procedimentos a seguir para garantir que a escola mantém ou recupera rapidamente os seus serviços essenciais perante uma interrupção significativa. A ativação do plano ocorre sempre que um incidente ultrapassa a capacidade de resolução imediata do Conselho Executivo, ou quando compromete a disponibilidade de sistemas críticos, como plataformas administrativas, redes internas, serviços de autenticação, bases de dados ou infraestruturas pedagógicas digitais. Estes critérios incluem falhas prolongadas de sistemas, ataques informáticos que afetem a integridade ou a confidencialidade dos dados, desastres físicos que impeçam o funcionamento normal das instalações ou qualquer situação que coloque em risco a continuidade das operações essenciais da escola.

Quando o plano é ativado, devem ser imediatamente contactadas as pessoas e organizações-chave, incluindo o Conselho Executivo, o coordenador TIC, a equipa de cibersegurança, a equipa de Ciber.Edu, o Encarregado de Proteção de Dados e, se necessário, entidades externas como fornecedores de serviços, equipas de suporte técnico e o Centro Nacional de Cibersegurança. Cada interveniente tem papéis e responsabilidades bem definidos: o Conselho Executivo valida a ativação e coordena a comunicação institucional, tendo as restantes equipas a finalidade de executar as ações técnicas de contenção e recuperação, o Encarregado de Proteção de Dados acompanha incidentes que envolvam dados pessoais e avalia obrigações legais de notificação, e os fornecedores externos prestam apoio especializado quando a resolução ultrapassa os recursos internos.

Os procedimentos de ativação incluem a confirmação do incidente, a avaliação inicial do impacto, a comunicação imediata aos responsáveis e a implementação das primeiras medidas de contenção. A partir desse momento, estabelece-se um fluxo de informação estruturado, garantindo que todas as decisões e atualizações são comunicadas de forma ordenada entre os departamentos envolvidos. A cadeia de comunicação deve assegurar que o Conselho Executivo recebe informação contínua sobre o estado da situação, coordenando as ações técnicas, informando os utilizadores apenas quando necessário, evitando alarmismo e garantindo clareza.

O plano de continuidade deve ainda prever instalações alternativas para situações em que os espaços físicos da escola estejam indisponíveis, permitindo que o Conselho Executivo e equipas responsáveis possam operar a partir de locais seguros e adequados. Da mesma forma, devem existir serviços alternativos que permitam manter funções essenciais, como plataformas de comunicação externas, redes temporárias, equipamentos de substituição ou soluções cloud que assegurem o acesso a dados críticos enquanto os sistemas principais são restaurados.

A mobilização de recursos internos e externos é uma parte fundamental do plano. Internamente, podem ser necessários equipamentos de reserva, acessos administrativos, documentação técnica e equipas adicionais de apoio. Externamente, podem ser acionados serviços de suporte especializado, empresas de recuperação de dados, fornecedores de software ou entidades públicas relevantes. A coordenação eficaz destes recursos garante que a resposta é rápida e que a recuperação decorre sem atrasos desnecessários.

Por fim, o plano deve incluir procedimentos claros para a reposição de sistemas ou serviços essenciais, definindo a ordem de recuperação, os métodos a utilizar, a validação da integridade dos dados restaurados e os testes necessários antes de restabelecer o funcionamento normal. A reposição deve ser realizada de forma controlada, garantindo que não subsistem vulnerabilidades e que os serviços recuperados são seguros e estáveis. Após a normalização, deve ser elaborado um relatório detalhado que permita avaliar o incidente, identificar melhorias e reforçar a resiliência da escola para situações futuras.

14. Definição de procedimentos de reação a incidentes

A definição de procedimentos de reação a incidentes estabelece a forma como a escola deve atuar sempre que ocorre um evento que comprometa, ou possa comprometer, a segurança da informação, a continuidade dos serviços ou a proteção de dados pessoais. Estes procedimentos garantem que a resposta é rápida, coordenada e eficaz, reduzindo o impacto do incidente e permitindo restaurar a normalidade com o mínimo de perturbação possível. Um incidente pode assumir várias formas, como uma falha de sistema, um ataque informático, a deteção de malware, o acesso não autorizado a

dados, a perda de equipamento ou qualquer situação que coloque em risco a integridade, a confidencialidade ou a disponibilidade da informação.

Quando um incidente é detetado, o primeiro passo consiste em reconhecê-lo e comunicá-lo de imediato, assegurando que a informação chega rapidamente às pessoas responsáveis pela gestão da situação. A prioridade inicial é conter o incidente, evitando que se propague ou cause danos adicionais. Esta contenção pode implicar o isolamento de equipamentos, a suspensão temporária de acessos, a desativação de contas comprometidas ou a interrupção de serviços específicos. Ao mesmo tempo, é recolhida informação relevante sobre o que aconteceu, quando ocorreu, que sistemas foram afetados e qual o possível impacto sobre dados pessoais ou serviços essenciais. Após a contenção, inicia-se a fase de análise e diagnóstico, na qual uma equipa responsável procura identificar a causa do incidente, avaliar a extensão dos danos e determinar as medidas necessárias para restaurar o funcionamento normal. Esta análise deve ser realizada de forma cuidadosa, garantindo que não se perdem evidências importantes para auditoria interna ou para eventual comunicação às autoridades competentes. Sempre que o incidente envolva dados pessoais, o Encarregado de Proteção de Dados deve ser informado e acompanhar o processo, avaliando a necessidade de notificar a Comissão Nacional de Proteção de Dados e os titulares afetados, conforme previsto no RGPD.

A fase seguinte consiste na recuperação dos sistemas e serviços afetados. Dependendo da gravidade do incidente, esta recuperação pode envolver a reposição de backups, a reinstalação de software, a substituição de equipamentos ou a reconfiguração de acessos e permissões. É fundamental garantir que os sistemas restaurados estão livres de vulnerabilidades e que não existe risco de recorrência imediata. Após a recuperação, os serviços são restabelecidos de forma controlada, garantindo que os utilizadores podem retomar as suas atividades com segurança.

Concluída a resolução técnica, procede-se ao registo detalhado do incidente, incluindo a descrição do ocorrido, as medidas tomadas, os tempos de resposta e os impactos identificados. Este registo é essencial para auditoria, para melhoria contínua e para reforçar a maturidade da escola em matéria de cibersegurança.

Finalmente, realiza-se uma avaliação pós-incidente, na qual se analisam as causas, se identificam fragilidades e se definem ações corretivas ou preventivas que permitam

evitar situações semelhantes no futuro. Esta reflexão pode levar à atualização de políticas internas, ao reforço de medidas técnicas, à formação de utilizadores ou à revisão dos planos de continuidade.