Plano Estratégico de Cibersegurança

E

Cronograma

1. Enquadramento e Objetivos Estratégicos

O presente documento estabelece um plano para a elevação da maturidade de cibersegurança do Agrupamento de Escolas (AE) de Silves. Atualmente, a instituição apresenta um nível de maturidade classificado como "Inicial", com uma gestão de segurança predominantemente "ad hoc", informal e reativa. É imperativo destacar que o cumprimento dos requisitos legais e regulamentares se fixa em apenas 1**/7** (Fonte: Identificar.pdf), o que exige uma intervenção imediata e estruturada. Este plano visa transitar de um estado de vulnerabilidade informal para um modelo de gestão resiliente, nível intermédio (onde as medidas são atingidas formalmente), focado em três objetivos fundamentais:

- **Conformidade Legal:** Atingir o pleno cumprimento das normas do Centro Nacional de Cibersegurança (CNCS) e regulamentações do setor educativo. Assegurar o pleno alinhamento com o **Regulamento de Proteção de Dados do AES**, garantindo que a modernização tecnológica e a gestão de ativos respeitem escrupulosamente os princípios da privacidade desde a conceção (*privacy by design*) e por defeito, conforme o RGPD e a Lei n.º 58/2019.
- **Continuidade de Serviço:** Formalizar e testar planos de recuperação que garantam a disponibilidade dos serviços críticos escolares.
- **Gestão de Ativos:** Estabelecer um controlo rigoroso e inventariado de todos os ativos lógicos e físicos que sustentam a atividade pedagógica e administrativa.

Como anexo a este relatório junta-se os resultados da aplicação da Ferramenta CyberCheckup.

2. Modelo de Governance e Responsabilidades

A atual indefinição de papéis constitui um risco elevado.
É instituída a seguinte matriz de responsabilidades, baseada na formalização de funções: Perfil/Função, Responsabilidade Principal em Cibersegurança.

Gestão de Topo: Compreensão formal das funções e responsabilidades de supervisão; aprovação de políticas e alocação de recursos (Ref: Proteger 1/7).

Responsáveis por Ativos: Associação obrigatória de um único responsável a cada ativo identificado. Esta responsabilidade é **indelegável** (Sugestão nº1).

Equipa Técnica (TI): Execução técnica da mitigação de vulnerabilidades, monitorização da capacidade produtiva e gestão sistemática de ativos.

Utilizadores Privilegiados: Aceitação formal e compreensão de papéis e responsabilidades acrescidas no acesso a sistemas críticos (Ref: Proteger 1/6).

Prestadores de Serviços: Cumprimento de requisitos mínimos de segurança e compromisso formal na deteção de eventos anómalos.

3. Requisitos de Gestão de Risco e Reporte de Incidentes

A capacidade de resposta do AE Silves depende da transição de canais informais para protocolos de comunicação estruturados.
REGRA DE OURO CNCS: É obrigatório o reporte de qualquer incidente de cibersegurança ao Centro Nacional de Cibersegurança (CNCS) num prazo máximo de **24 horas** após a sua deteção.
Para garantir o cumprimento desta norma, os passos de escalonamento são:

1. **Classificação de Impacto:** Avaliação imediata do evento com base em critérios de impacto pré-definidos, corrigindo a atual lacuna de classificação (Ref: Detetar 1/3).
2. **Investigação Técnica:** Verificação das notificações dos sistemas de deteção para confirmar o método de ataque e o alvo.
3. **Ativação do Plano de Comunicação:** Notificação das audiências internas e externas através dos canais formais estabelecidos (superando a atual natureza reativa).
4. **Reporte Externo:** Submissão obrigatória de informação ao CNCS e coordenação com partes interessadas externas identificadas.

4. Estratégia de Melhoria por Domínios (NIST/CyberCheckup)

As ações seguintes derivam diretamente das recomendações para colmatar as deficiências identificadas no CyberCheckup:

1.Identificar

- **Inventário e Responsabilidade:** Registo individual e sistemático de ativos com identificação de responsáveis únicos.
- **Mapeamento de Processos:** Identificação de ativos que suportam processos críticos em sistema de gestão consolidado.
- **Monitorização de Capacidade:** Registo e monitorização da capacidade produtiva de infraestrutura, redes e sistemas (Sugestão nº2).

2.Proteger

- **Gestão de Identidades (IAM):** Criação de uma base única de identidades e regras de acesso baseadas no princípio do menor privilégio.
- **Segurança de Acessos:** Centralização tecnológica do controlo de acessos remotos e integração com sistemas de acesso físico.
- **Manutenção e Suportes:** Implementação de processos formais para revisão e aprovação de manutenções remotas (Ref: Proteger 1/22) e proteção rigorosa de suportes de dados amovíveis (Ref: Proteger 1/23).

3.Detetar

- **Proatividade:** Transição da deteção de código malicioso de um estado reativo (Ref: Detetar 1/7) para uma monitorização proativa e sistemática.
- **Gestão de Fornecedores:** Avaliação regular das permissões concedidas a prestadores de serviços e compromisso destes na deteção de anomalias (Sugestão nº3).
- **Vulnerabilidades:** Implementação de deteção automática de vulnerabilidades em ativos críticos (Ref: Detetar 1/9).

4.Responder

- **Análise Técnica:** Realização de análises técnicas de ameaças recorrentes e avaliação formal da eficiência dos sistemas de antivírus (Sugestão nº1).
- **Resposta Integrada:** Documentação e teste de procedimentos integrados de tratamento de incidentes para reduzir o impacto operacional.

5.Recuperar

- **Continuidade de Negócio:** Registo e teste de planos de continuidade especificamente adaptados ao âmbito do AE Silves (Sugestão nº4).
- **Gestão de Cópias de Segurança:** Estabelecimento de um processo formal de gestão e teste de cópias de segurança (backups), abandonando práticas ad hoc.

5. Cronograma de Implementação (6 Meses)

Mês - Atividades Principais - Entregável

Mês 1 e 2: Identificação e Governação

- **Atividade 1: Inventariação Sistemática de Ativos.**
    - **Procedimento Técnico:** Utilizar uma ferramenta de gestão integrada para registar todos os dispositivos físicos, redes e software. Cada ativo deve ter um identificador individual, classificação de criticidade e um único responsável associado. Mapear fluxos de dados e comunicações ao nível do IP [1].
    - **Responsável:** Equipa de TI e Gestores de Ativos.
- **Atividade 2: Formalização da Política de Segurança.**
    - **Procedimento Técnico:** Redigir e divulgar internamente a Política de Segurança, integrando os requisitos legais e regulamentares aplicáveis.
    - **Responsável:** Gestão de Topo e Consultoria de Segurança.

Mês 2 e 3: Proteção e Controlo de Acessos

- **Atividade 1: Gestão de Identidades e Acessos (IAM).**
    - **Procedimento Técnico:** Criar uma **base única de identidades** com regras transversais. Implementar o **princípio do menor privilégio**, garantindo que utilizadores com acessos privilegiados compreendam formalmente as suas responsabilidades.
    - **Responsável:** Administradores de Sistemas.
- **Atividade 2: Segurança de Acessos Remotos.**
    - **Procedimento Técnico:** Centralizar os acessos remotos através de soluções tecnológicas que apliquem segurança específica (ex: VPNs cifradas ou MFA) e integrar com o sistema transversal de identidades.
    - **Responsável:** Equipa de Redes e Segurança.

Mês 4: Deteção e Monitorização

- **Atividade 1: Centralização de Eventos e Monitorização.**
    - **Procedimento Técnico:** Configurar um sistema centralizado para coleta e correlação de eventos de segurança de várias fontes. Implementar padrões

[1] Possíveis ferramentas: • **GLPI** ou **Snipe-IT**: Soluções de código aberto (open-source) muito utilizadas para inventário de hardware e software. • **Lansweeper**: Focada na descoberta automática de ativos na rede. • **ServiceNow** ou **Jira Service Management**: Plataformas mais abrangentes para organizações de maior dimensão.

de monitorização para comportamentos anómalos e monitorizar regularmente as atividades de prestadores de serviços externos.

    - **Responsável:** Equipa de Operações de Segurança (SOC) / Técnicos de TI.

- **Atividade 2: Verificação de Integridade.**
    - **Procedimento Técnico:** Implementar mecanismos para verificar a integridade de software, firmware e dados, garantindo que os processos de deteção instalados sejam fiáveis.
    - **Responsável:** Técnicos de Sistemas.

Mês 5 e 6: Resposta, Recuperação e Resiliência

- **Atividade 1: Formalização do Plano de Resposta a Incidentes.**
    - **Procedimento Técnico:** Estabelecer procedimentos de resposta integrada, definindo critérios de reporte e canais de comunicação. **Obrigatório:** Garantir a capacidade de reportar incidentes relevantes ao **CNCS no prazo máximo de 24 horas**.
    - **Responsável:** Gestão de Topo e Equipa de Resposta a Incidentes (CSIRT local).
- **Atividade 2: Plano de Continuidade e Backups.**
    - **Procedimento Técnico:** Implementar regras formais para a realização, manutenção e teste de **cópias de segurança**. Registar e testar os planos de continuidade e recuperação para garantir a resiliência dos sistemas críticos.
    - **Responsável:** Equipa de TI e Gestão de Topo.

Requisitos Obrigatórios de Gestão de Risco e Reporte

De acordo com os princípios do regime jurídico integrados nestas atividades:

1. **Avaliação de Impacto:** Todos os incidentes detetados devem ter o seu impacto classificado formalmente para determinar a necessidade de reporte externo.
2. **Comunicação Integrada:** Deve ser estabelecido um plano de comunicação que identifique as audiências adequadas (internas e externas) e o propósito de cada mensagem durante uma crise.
3. **Monitorização de Vulnerabilidades:** As vulnerabilidades identificadas devem ser analisadas regularmente e mitigadas ou documentadas como riscos aceites pela gestão.

6. Considerações Finais sobre Conformidade

A transição do conhecimento informal e "ad hoc" para o registo formal e sistemático é a única via para garantir a sustentabilidade do Agrupamento de Escolas de Silves.
A superação do atual score de conformidade de 1**/7** é uma prioridade absoluta.
Este plano não representa um projeto isolado, mas sim o início de um ciclo de resiliência contínua, onde a proteção da comunidade educativa e a integridade dos dados são pilares inalienáveis da missão da instituição.

Documentos decorrentes do Plano Estratégico de Cibersegurança datado de 17-04-2026:

- Política de Segurança da Informação
- Plano de Resposta a Incidentes de Segurança (Documento orientador)
- Política de Boas práticas de mitigação da segurança digital (Ações concretas)

- Política de Gestão de Acessos
- Política de Backup e Recuperação de Dados
- Política de Utilização Aceitável dos Sistemas de Informação
- Procedimentos de Gestão de Equipamentos e Sistemas.
- Procedimentos de Monitorização e Registo de Atividades
- Plano de Continuidade e Recuperação de Serviços
- Plano de Sensibilização e Formação em Segurança da Informação

Data
O Diretor

ANEXOS

Resultados da aplicação da Ferramenta CyberCheckup ao AES