Política de Segurança da Informação

(Classificação do documento: Uso interno)

Documento	Política de Segurança da Informação AES
Equipa	Proteção de Dados e Conformidade com a Informação
Tipo	Escola/Política
Versão	1.0
Data	04-2026
Responsável	**Equipa cibersegurança escolar** - Tito Mendes - Nuno Garção - Jorge Lopes - Mónica Franco - Helder Oliveira - Graça Santos
Aprovado por	Direção do Agrupamento
Próxima revisão	2027

Índice

Política da Segurança da Informação do Agrupamento de Escolas de Silves (AES)

O Agrupamento de Escolas de Silves reconhece que a informação é um recurso essencial para o cumprimento da sua missão educativa e para a concretização dos seus objetivos estratégicos. Tal como as pessoas que integram a comunidade educativa, a informação constitui um dos ativos mais importantes da organização.

A presente Política de Segurança da Informação tem como objetivo assegurar a proteção adequada da informação, prevenindo situações que possam comprometer a sua confidencialidade, integridade ou disponibilidade. A ausência de mecanismos de proteção adequados pode originar impactos relevantes ao nível operacional, legal, financeiro ou reputacional para o agrupamento.

Este documento estabelece os princípios e orientações gerais para a gestão da segurança da informação no Agrupamento de Escolas de Silves, bem como identifica um conjunto de políticas e procedimentos complementares que, em conjunto, constituem o sistema de segurança da informação da organização.

1. Qual é o objetivo da Política de Segurança da Informação?

A Política de Segurança da Informação tem como objetivo estabelecer os princípios e orientações que garantem a proteção adequada da informação e dos sistemas de informação do Agrupamento de Escolas.

Em particular, pretende:

1.1. Garantir que o tratamento de toda a informação digital ou física no Agrupamento seja realizado em conformidade com o **Regulamento de Proteção de Dados do AES**, assegurando a proteção dos direitos e liberdades dos alunos, docentes e funcionários.

1.2. Garantir que toda a informação e os sistemas de informação utilizados pelo Agrupamento são protegidos de forma adequada, em conformidade com as políticas internas e com a legislação aplicável.

1.3. Assegurar que a informação apenas é disponibilizada a utilizadores que possuam autorização legítima para o seu acesso.

1.4. Promover um ambiente seguro e fiável de utilização dos sistemas de informação para docentes, alunos, funcionários e outros utilizadores autorizados.

1.5. Reduzir o risco de utilização indevida da informação ou dos sistemas informáticos, prevenindo potenciais impactos operacionais, legais, financeiros ou reputacionais para o Agrupamento.

1.6. Garantir que todos os utilizadores têm conhecimento desta política e das restantes normas associadas, assegurando igualmente o cumprimento da legislação aplicável em matéria de proteção de dados e segurança da informação, nomeadamente do **Regulamento Geral sobre a Proteção de Dados (RGPD)** — General Data Protection Regulation — e das diretivas europeias relativas à segurança das redes e sistemas de informação, em particular a NIS2 Directive.

1.7. Promover a consciencialização dos utilizadores relativamente às suas responsabilidades na proteção da confidencialidade, integridade e disponibilidade da informação que tratam.

1.8. Assegurar que quaisquer incidentes ou violações de segurança da informação são devidamente reportados e tratados de acordo com os procedimentos definidos pelo Agrupamento.

1.9. Demonstrar o compromisso da Direção do Agrupamento com a segurança da informação, definindo responsabilidades claras na proteção da informação e dos sistemas de informação.

2. Qual é a Política de Segurança da Informação do Agrupamento?

A Política de Segurança da Informação do Agrupamento estabelece um conjunto de princípios e medidas destinadas a garantir a proteção da informação e dos sistemas de informação utilizados pela organização.

Classificação da Informação

2.1. Toda a informação produzida ou tratada pelo Agrupamento deve ser classificada e protegida de acordo com o seu nível de sensibilidade e risco.

Para efeitos de gestão da informação, poderão ser consideradas as seguintes categorias:

Confidencial (nível 4) – Informação sensível que apenas pode ser acedida por utilizadores autorizados (por exemplo, dados pessoais de alunos, funcionários ou processos administrativos).

Restrito (nível 3) - Informação cuja divulgação não autorizada, embora não cause danos críticos imediatos, pode comprometer a eficácia de processos operacionais, pedagógicos ou administrativos específicos do Agrupamento (por exemplo, atas de reuniões de conselhos de turma ou pedagógicos, listas de alunos para fins específicos de projetos internos, detalhes técnicos de infraestrutura de rede, ou planeamento estratégico de exames e avaliações).
Uso interno (nível 2) – Informação destinada à utilização interna do Agrupamento e que não deve ser divulgada externamente sem autorização (por exemplo, circulares informativas, minutas administrativas e manuais de procedimentos internos que, servindo apenas o funcionamento operacional do Agrupamento, não podem ser divulgados externamente sem autorização formal da direção para proteger os processos escolares).
Pública (nível 1) – Informação que pode ser divulgada publicamente sem restrições (por exemplo, informação disponível no website institucional).

Controlos de Segurança

2.2. Os sistemas de informação do Agrupamento devem ser configurados com mecanismos de segurança adequados, incluindo atualizações de software, antivírus, firewall e outras medidas de proteção.

2.3. O acesso aos sistemas de informação deve ser gerido através de contas individuais e de permissões adequadas às funções de cada utilizador.

Utilização de Dispositivos Pessoais (BYOD)

2.4. A utilização de dispositivos pessoais (como computadores portáteis, tablets ou smartphones) para acesso aos sistemas ou redes do Agrupamento deve cumprir as regras de segurança definidas pela organização.

Sempre que aplicável, os dispositivos devem:

- possuir sistemas atualizados
- utilizar mecanismos de proteção adequados
- respeitar as políticas de acesso definidas pelo Agrupamento.

Utilização da Rede Wi-Fi

2.5. O acesso às redes sem fios do Agrupamento deve ser realizado de acordo com as regras definidas para cada rede disponível (administrativa, professores e alunos).

A utilização da rede Wi-Fi deve respeitar as normas de segurança estabelecidas e não pode ser utilizada para atividades ilícitas ou que comprometam a segurança dos sistemas de informação.

Disponibilidade da Informação

2.6. Devem existir mecanismos de backup e procedimentos de recuperação que permitam minimizar o risco de perda de dados ou interrupção de serviços considerados críticos para o funcionamento do Agrupamento.

Monitorização

2.7. O Agrupamento poderá realizar monitorização técnica dos sistemas de informação com o objetivo de garantir o seu correto funcionamento e proteger os sistemas contra vírus, ataques informáticos ou outras ameaças conhecidas.
Esta monitorização destina-se apenas à proteção dos sistemas e não implica, em condições normais, a análise do conteúdo das comunicações individuais dos utilizadores.

2.8. O Agrupamento reserva-se o direito de monitorizar a utilização dos seus sistemas de informação sempre que tal seja necessário para garantir a segurança, a integridade e o funcionamento adequado dos sistemas.

Incidentes de Segurança

2.9. Qualquer utilizador que suspeite de uma falha ou incidente de segurança deve comunicar a situação à equipa responsável pelos sistemas de informação do Agrupamento.

2.10. Sempre que exista suspeita de comprometimento de sistemas ou contas de utilizador, o Agrupamento poderá proceder à suspensão temporária de acessos ou ao isolamento de sistemas afetados, de forma a prevenir a propagação do incidente.

2.11. O Agrupamento deve manter procedimentos para resposta a incidentes de segurança da informação, os quais devem ser testados e revistos periodicamente.

2.12. Sempre que um incidente de segurança envolva dados pessoais, deverá ser garantido o cumprimento das obrigações legais aplicáveis, nomeadamente as previstas no **Regulamento Geral sobre a Proteção de Dados (RGPD)**.

2.13. Incidentes relacionados com a segurança física de equipamentos ou instalações devem ser comunicados à Direção ou aos serviços responsáveis pela segurança do Agrupamento.

Sensibilização e Cumprimento da Política

2.14. A presente política deve ser divulgada a todos os utilizadores dos sistemas de informação do Agrupamento.

2.15. Todos os utilizadores devem conhecer e cumprir as regras definidas nesta política.

2.16. O Agrupamento promoverá ações de sensibilização e formação em segurança da informação sempre que considerado necessário.

2.17. O incumprimento desta política poderá resultar na limitação ou suspensão do acesso aos sistemas de informação e poderá dar origem à aplicação de medidas disciplinares, de acordo com a legislação aplicável.

3. Âmbito da Política

A presente secção define os utilizadores, serviços, sistemas e tipos de informação abrangidos pela Política de Segurança da Informação.

3.1. A presente Política de Segurança da Informação aplica-se a todos os utilizadores que acedem ou utilizam informação e sistemas de informação do Agrupamento de Escolas, incluindo:

- docentes
- alunos
- assistentes técnicos e operacionais
- membros da direção
- colaboradores externos
- prestadores de serviços
- quaisquer outras entidades que tenham acesso autorizado aos sistemas ou à informação do Agrupamento.

Ao longo deste documento, estes intervenientes são designados genericamente por **utilizadores**.

3.2. Para efeitos desta política, consideram-se abrangidos todos os serviços, departamentos, estabelecimentos de ensino e estruturas administrativas que integram o Agrupamento de Escolas.

3.3. Esta política aplica-se à informação em todas as suas formas e suportes, incluindo:

- informação digital armazenada em sistemas informáticos
- documentos em suporte papel
- informação transmitida por meios eletrónicos (email, plataformas digitais, redes informáticas)
- informação transmitida por outros meios de comunicação, incluindo comunicações telefónicas.

Abrange igualmente diferentes tipos de conteúdo, tais como texto, imagens, áudio, vídeo e dados utilizados em sistemas de processamento automatizado de informação ou ferramentas digitais.

A política aplica-se durante todo o ciclo de vida da informação, desde a sua criação ou recolha, passando pelo armazenamento e utilização, até à sua eliminação ou arquivo.

Inclui igualmente informação tratada através de serviços cloud, plataformas educativas ou ferramentas digitais utilizadas pelo Agrupamento.

3.4. A segurança da informação baseia-se na proteção dos seguintes princípios fundamentais:
Confidencialidade: Garantir que a informação apenas é acessível a pessoas autorizadas.
Integridade: Garantir a exatidão e a completude da informação, prevenindo alterações indevidas.
Disponibilidade: Garantir que a informação e os sistemas associados estão disponíveis para os utilizadores autorizados sempre que necessário.

4. Responsabilidades

4.1. Todos os utilizadores dos sistemas de informação do Agrupamento são responsáveis por conhecer e cumprir a presente Política de Segurança da Informação, bem como as restantes normas e procedimentos associados e a legislação aplicável.

4.2. O Diretor do Agrupamento é responsável por assegurar que existem condições organizacionais e recursos adequados para a implementação das medidas de segurança da informação.
Compete igualmente ao Diretor aprovar a presente política e garantir a sua aplicação no âmbito do Agrupamento.

4.3. A coordenação e/ou equipa de Cibersegurança e a equipa responsável pelas Tecnologias de Informação e Comunicação (TIC) do Agrupamento é responsável por:

- apoiar a implementação das medidas de segurança da informação

- manter e atualizar esta política e os procedimentos associados
- monitorizar o funcionamento dos sistemas de informação
- coordenar a resposta a incidentes de segurança.

4.4. Sempre que necessário, os responsáveis pelos serviços ou departamentos do Agrupamento devem colaborar na implementação das medidas de segurança e na gestão adequada da informação sob a sua responsabilidade.

4.5. A presente Política de Segurança da Informação deverá ser revista periodicamente, pelo menos uma vez por ano, ou sempre que ocorram alterações relevantes nos sistemas de informação, na legislação aplicável ou na estrutura organizacional do Agrupamento.

5. Políticas e procedimentos associados

A presente Política de Segurança da Informação é suportada por um conjunto de políticas e procedimentos complementares que estabelecem regras específicas para diferentes áreas da segurança da informação no Agrupamento de Escolas (Política de Boas práticas de mitigação da segurança digital e Plano de Resposta a Incidentes de Segurança).

Estes documentos, em conjunto, constituem o sistema de gestão de segurança da informação do Agrupamento.

Entre as principais políticas e procedimentos associados incluem-se:

5.1. **Política de Gestão de Acessos:** Define as regras para criação, gestão e revogação de contas de utilizador, bem como os níveis de acesso aos sistemas de informação.

5.2. **Política de Backup e Recuperação de Dados:** Estabelece os procedimentos para a realização de cópias de segurança e para a recuperação de dados em caso de falha ou incidente.

5.3. **Política de Utilização Aceitável dos Sistemas de Informação:** Define as regras de utilização dos sistemas, redes e equipamentos informáticos do Agrupamento por parte de alunos, docentes, funcionários e outros utilizadores.

5.4. **Procedimentos de Gestão de Equipamentos e Sistemas:** Define as regras de configuração, atualização e manutenção dos sistemas informáticos e equipamentos de rede.

5.5. **Procedimentos de Monitorização e Registo de Atividades:** Estabelece os mecanismos de monitorização dos sistemas de informação e a gestão de registos de atividade (logs) para deteção de incidentes de segurança.

5.6. **Plano de Continuidade e Recuperação de Serviços:** Define as medidas destinadas a assegurar a continuidade dos serviços essenciais do Agrupamento em caso de falha grave ou incidente.

5.7. **Plano de Sensibilização e Formação em Segurança da Informação:** Define as ações de formação e sensibilização destinadas a promover boas práticas de segurança entre os utilizadores dos sistemas de informação.

5.8. **Plano de Resposta a Incidentes de Segurança:** Define os procedimentos para identificação, comunicação e resposta a incidentes de segurança da informação.

6. Legislação e normas aplicáveis

6.1. Legislação aplicável

A utilização e tratamento da informação no Agrupamento de Escolas devem cumprir a legislação aplicável em matéria de proteção de dados, segurança da informação e utilização de sistemas informáticos.

Todos os utilizadores têm a obrigação de cumprir a legislação em vigor, incluindo, mas não se limitando a:

- **Regulamento Geral sobre a Proteção de Dados (RGPD):** General Data Protection Regulation
- **Regulamento de Proteção de Dados do Agrupamento de Escolas de Silves**
- **Diretiva NIS2 relativa à segurança das redes e sistemas de informação**: Diretiva NIS2 (Diretiva (UE) 2022/2555)
- **Lei do Cibercrime (Lei n.º 109/2009)**
- **Lei de Acesso aos Documentos Administrativos (Lei n.º 26/2016)**
- **Código do Direito de Autor e dos Direitos Conexos (Decreto-Lei n.º 63/85)**
- **Lei da Proteção de Dados Pessoais (Lei n.º 58/2019)**

6.2. Políticas e documentos internos relacionados

A presente Política de Segurança da Informação é complementada por um conjunto de políticas e procedimentos internos que suportam a gestão da segurança da informação no Agrupamento, incluindo:

- Plano Estratégico e Cronograma de Cibersegurança AE Silves (Enquadramento)

- Plano de Resposta a Incidentes de Segurança

- 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

Assinado por: **Tito Romeu Gomes de Sousa Maia Mendes**
Num. de Identificação: 10543080
Data: 2026.05.22 16:36:27+01'00'
Certificado por: **Diário da República**
Atributos certificados: **Diretor - Agrupamento de Escolas de Silves**