ALBERGARIA-A-VELHA
MUNICÍPIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Versão 1.0

Aprovado em 2026-…..-….

SUMÁRIO

1. Objetivo....3
2. Princípios....4
3. Âmbito....4
4. Partes interessadas....5
5. Compromissos....5
6. Gestão da Segurança da Informação e Cibersegurança....6
7. Medidas de Segurança da Informação e Cibersegurança....7
8. Gestão de Incidentes de Segurança....8
9. Formação e sensibilização....8
10. Comunicação, Divulgação, Revisão e Aprovação....9
11. Registo de revisão....9

POLÍTICA DE SEGURANÇA
DA INFORMAÇÃO E CIBERSEGURANÇA

1. Objetivo

A presente Política de Segurança da Informação e Cibersegurança estabelece os princípios, orientações e compromissos do Município de Albergaria-a-Velha relativos à proteção da informação, das redes e dos sistemas de informação que suportam a sua atividade e a prestação de serviços públicos.

A informação, nos seus diversos formatos e suportes, é reconhecida como um bem de elevado valor institucional, operacional e legal, cuja proteção adequada é indispensável para garantir:

- A continuidade dos serviços essenciais prestados à comunidade local;
- A confiança dos munícipes e das entidades parceiras;
- O cumprimento das obrigações legais, regulamentares e contratuais, nomeadamente as que decorrem do Regime Jurídico da Cibersegurança, versão vigente, do Regulamento Geral sobre a Proteção de Dados (RGPD), dos regimes aplicáveis à gestão, classificação, avaliação, conservação e acesso à informação arquivística e demais legislação nacional aplicável;
- A salvaguarda dos direitos fundamentais dos titulares dos dados pessoais tratados pelo Município.

Esta política visa, ainda, garantir que os princípios de segurança da informação — confidencialidade, integridade, disponibilidade, autenticidade e resiliência — estão devidamente integrados na estratégia, cultura e operação do Município, promovendo uma abordagem baseada no risco e na melhoria contínua.

No atual contexto de crescente digitalização dos serviços Municipais, e da subsequente dependência de tecnologias de informação, para a execução das suas competências, torna-se essencial reconhecer o aumento significativo da exposição ao ciberespaço. Tal realidade, potencia a existência de novas vulnerabilidades e subsequentes ameaças e riscos que exigem uma resposta institucional robusta, coordenada e sustentada numa política clara de segurança da informação e cibersegurança.

Neste enquadramento, o Município de Albergaria-a-Velha definiu, aprovou e comunica formalmente a presente Política de Segurança da Informação e Cibersegurança como expressão do seu compromisso inequívoco com a proteção da informação, a resiliência digital dos seus serviços e o cumprimento rigoroso das obrigações legais e regulamentares aplicáveis.

Esta Política articula-se com um conjunto de políticas, normas e procedimentos complementares, orienta a atuação de todos os intervenientes e constitui um instrumento de governação fundamental para a gestão da segurança da informação e cibersegurança no Município.

2. Princípios

A gestão da segurança da informação e cibersegurança do Município rege-se pelos princípios da legalidade, proporcionalidade, responsabilidade, prevenção, gestão do risco, necessidade de conhecer e melhoria contínua. Assume-se, de igual modo, o compromisso com a preservação do valor legal e probatório da informação, assegurando que os controlos de segurança garantem a autenticidade, integridade, não-repúdio e usabilidade dos documentos ao longo de todo o seu ciclo de vida.

A segurança da informação e a cibersegurança constituem uma responsabilidade partilhada por todos os intervenientes que acedem, utilizam, administram ou tratam informação, redes, sistemas de informação ou outros ativos do Município.

A proteção deve ser adequada à criticidade da informação, dos ativos e dos serviços suportados, tendo em consideração os riscos identificados e os requisitos legais, regulamentares e contratuais aplicáveis.

3. Âmbito

A presente Política aplica-se a todo o ecossistema informacional do Município de Albergaria-a-Velha, incluindo os ativos físicos e digitais que suportam os serviços essenciais prestados à comunidade local, nomeadamente sistemas de informação, bases de dados, equipamentos, infraestruturas tecnológicas, redes de comunicação e processos organizacionais.

Estão incluídas todas as atividades de recolha, tratamento, armazenamento, transmissão e eliminação de informação associadas à operação dos serviços municipais.

Esta política é aplicável a:

- Eleitos locais e titulares de cargos dirigentes;
- Todos os trabalhadores do Município, independentemente do vínculo contratual;
- Prestadores de serviços, fornecedores, entidades subcontratadas e outros parceiros externos com acesso a sistemas ou informação municipal;
- Entidades públicas e privadas que utilizem ou integrem sistemas sob gestão do Município;
- Demais utilizadores autorizados dos ativos e serviços abrangidos.
- O acesso e utilização dos ativos do Município pressupõem o cumprimento das políticas, normas, processos e procedimentos de segurança aplicáveis, sem prejuízo das consequências disciplinares, contratuais ou legais que possam resultar do respetivo incumprimento.

4. Partes interessadas

Entende-se como partes interessadas todas as pessoas, instituições públicas ou privadas que interagem com o âmbito de proteção para a Segurança da Informação e Cibersegurança.

No contexto da presente política, identificam-se:

- Partes interessadas internas – Eleitos locais, trabalhadores detentores dos vários vínculos laborais previstos na Lei Geral do Trabalho em Funções Públicas.
- Partes interessadas externas – Administração Pública Central de tutela às autarquias locais; Entidades reguladoras – Centro Nacional de Cibersegurança; Comissão Nacional de Proteção de Dados; ERSAR - Entidade Reguladora dos Serviços de Águas e Resíduos; Munícipes; Agrupamentos escolares do concelho; Juntas de freguesia do Concelho; Pessoas singulares ou entidades com interesses no âmbito da geografia do Município; Comunidade Intermunicipal da Região de Aveiro; Associações sem fins lucrativos do concelho; Instituições privadas de solidariedade social do concelho; Prestadores de Serviços/Avençados; Prestadores de Serviços/fornecedores.

Para cada caso, serão analisados os requisitos de segurança que constam em legislação, regulamentação, contratos, protocolos ou outros compromissos firmados com o Município.

5. Compromissos

O Município de Albergaria-a-Velha assume o compromisso de proteger a informação, as redes e os sistemas de informação sob a sua responsabilidade e de promover um nível de cibersegurança adequado aos riscos associados à sua atividade.

Para esse efeito, o Município compromete-se a:

- proteger a confidencialidade, integridade, disponibilidade e autenticidade da informação;
- identificar, analisar, avaliar e tratar os riscos de segurança da informação e cibersegurança;
- implementar as medidas de cibersegurança aplicáveis de acordo com o quadro legal e regulamentar vigente;
- proteger os ativos contra acessos, utilizações, alterações, divulgações, perdas ou destruições não autorizadas;
- promover a continuidade e a resiliência das redes, sistemas de informação e serviços municipais;
- prevenir, detetar, responder e recuperar de incidentes de cibersegurança;
- integrar requisitos de segurança na gestão de fornecedores, prestadores de serviços e demais terceiros relevantes;
- promover a sensibilização, formação e responsabilização dos utilizadores;
- monitorizar e avaliar a adequação e eficácia das medidas implementadas;
- promover a melhoria contínua da segurança da informação e cibersegurança;
- assegurar os recursos adequados ao cumprimento das medidas de cibersegurança e demais obrigações aplicáveis.

As medidas adotadas são adequadas ao risco, à criticidade dos ativos, à natureza da informação e aos requisitos legais, regulamentares e contratuais aplicáveis.

6. Gestão da Segurança da Informação e Cibersegurança

A implementação e coordenação das medidas de segurança da informação e cibersegurança são asseguradas pelas unidades orgânicas e funções competentes do Município, de acordo com as responsabilidades que lhes estejam atribuídas.

O Município assegura a disponibilização dos recursos adequados ao cumprimento das medidas de cibersegurança aplicáveis e das restantes obrigações decorrentes do Regime Jurídico da Cibersegurança e respetiva regulamentação.

Sempre que aplicável e legalmente exigível, o Município procede à designação e comunicação às autoridades competentes das funções, pontos de contacto ou outros elementos de articulação previstos no quadro legal e regulamentar aplicável.

Os titulares de cargos dirigentes integram os requisitos e práticas de segurança da informação e cibersegurança na gestão das áreas e recursos sob a sua responsabilidade.

Os utilizadores cumprem as políticas, normas, processos e procedimentos que lhes sejam aplicáveis e participam nas ações de sensibilização e formação estabelecidas pelo Município.

A gestão da segurança da informação e cibersegurança assenta numa abordagem baseada no risco e numa perspetiva sistémica que integra pessoas, processos e tecnologia sob a liderança ativa da gestão de topo, sendo complementada por mecanismos de monitorização, avaliação, verificação, auditoria e revisão.

As políticas, normas, processos e procedimentos são documentados, mantidos e atualizados de acordo com as necessidades do Município e com os requisitos aplicáveis.

7. Medidas de Segurança da Informação e Cibersegurança

As medidas de segurança da informação e de cibersegurança implementadas pelo Município são definidas com base em avaliações sistemáticas de risco e nas melhores práticas nacionais e internacionais, nomeadamente a norma ISO/IEC 27001 e o Quadro Nacional de Referência para a Cibersegurança, articulando a salvaguarda operacional imediata com as diretrizes de preservação digital de longo prazo.

O Município compromete-se a alocar os recursos humanos, técnicos e financeiros necessários para garantir a implementação, manutenção e melhoria contínua destas medidas, assegurando que os controlos técnicos, organizacionais e procedimentais permanecem eficazes perante ameaças e vulnerabilidades emergentes.

Estas medidas abrangem, de forma especial, a proteção dos serviços essenciais e dos ativos/recursos associados quando expostos ao ciberespaço, prevenindo e mitigando riscos decorrentes de ciberataques, bem como a gestão da segurança na cadeia de abastecimento, assegurando que fornecedores, prestadores de serviços e parceiros externos cumprem padrões de segurança compatíveis com os do Município.

As medidas são objeto de monitorização permanente e de auditorias periódicas, permitindo avaliar a sua eficácia e introduzir melhorias sempre que necessário, de forma a assegurar a confidencialidade, integridade, disponibilidade, privacidade, não repúdio e resiliência da informação e dos sistemas que a suportam.

8. Gestão de Incidentes de Segurança

O Município estabelece e mantém processos e procedimentos para a identificação, deteção, registo, análise, tratamento, resposta e recuperação de incidentes de cibersegurança.

Os incidentes são avaliados em função da sua natureza, gravidade e impacto, sendo adotadas as medidas adequadas para limitar os seus efeitos, recuperar os serviços afetados e reduzir a probabilidade ou impacto da sua recorrência.

Os incidentes abrangidos por obrigações de notificação são comunicados às autoridades competentes nos termos, condições e prazos previstos no quadro legal e regulamentar aplicável.

Sempre que aplicável, são igualmente asseguradas as comunicações a outras entidades ou partes interessadas decorrentes de obrigações legais, regulamentares ou contratuais.

As conclusões resultantes da análise de incidentes são consideradas nos processos de gestão do risco e de melhoria contínua da segurança da informação e cibersegurança.

9. Formação e sensibilização

O Município promove uma cultura de segurança da informação e cibersegurança baseada no conhecimento, prevenção e responsabilidade dos seus intervenientes.

Para esse efeito, são estabelecidas ações de sensibilização e formação em cibersegurança adequadas às funções, responsabilidades e riscos associados aos respetivos destinatários, promovendo o desenvolvimento de uma cultura de responsabilidade cívica ativa.

O Município estabelece e mantém um plano de formação em cibersegurança e os processos e procedimentos necessários à sua implementação, de acordo com as medidas de cibersegurança aplicáveis.

A participação nas ações definidas como obrigatórias pelo Município deve ser assegurada pelos respetivos destinatários.

As atividades de sensibilização e formação são objeto de acompanhamento e avaliação, sendo os respetivos resultados considerados, quando aplicável, na melhoria das medidas de cibersegurança.

10. Comunicação, Divulgação, Revisão e Aprovação

A presente Política é de natureza pública e será divulgada a todas as partes interessadas através dos canais de comunicação institucionais do Município, em formato não editável, garantindo a sua acessibilidade e integridade.

O Município compromete-se a rever e atualizar este documento sempre que se verifiquem alterações relevantes no enquadramento legal, regulamentar ou tecnológico, ou sempre que sejam identificadas necessidades de melhoria decorrentes de auditorias, incidentes ou mudanças organizacionais.

A atualização da Política seguirá um processo formal de aprovação pelo Executivo Municipal, assegurando que todas as versões são devidamente controladas e substituem integralmente as anteriores. Após cada revisão, a nova versão será novamente comunicada a todos os destinatários abrangidos, reforçando a importância do seu conhecimento e cumprimento.

Registo de revisão

Versão	Motivo da revisão	Elaborado por	Aprovado por	Data aprovação
1.0	Aprovação	Câmara Municipal		