POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

MUNICÍPIO PONTE DE LIMA
TERRA RICA DA HUMANIDADE

Índice

1. OBJETIVO DA POLÍTICA

A informação é considerada, pelo Município de Ponte de Lima, como um ativo estratégico, fundamental e de considerável valor para a operacionalidade dos serviços disponibilizados a toda a comunidade, na prossecução das competências atribuídas à autarquia.

O Município de Ponte de Lima entende como fundamental a definição e aplicação de uma política que defina os seus compromissos para a proteção dessa informação, tendo designado um Responsável pela Segurança que assegure a gestão da segurança da informação e da respetiva Cibersegurança.

O Responsável de Segurança deve garantir que esta política se mantém adequada para os objetivos estratégicos do Município e que esteja devidamente integrada no respetivo Plano de Segurança.

O Município de Ponte de Lima compromete-se a disponibilizar os necessários recursos e suporte, bem como levará a cabo a missão de garantir a melhoria contínua de tais compromissos e respetivas métricas de eficácia, por forma a assegurar a conformidade para com os requisitos legais e as expectativas e requisitos de segurança identificados pelas partes interessadas desta instituição.

2. ÂMBITO DE PROTEÇÃO PARA A SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

O âmbito de proteção para a Segurança da Informação e respetiva Cibersegurança inclui os serviços essenciais do Município, assim como os ativos e recursos que sustentam a sua utilização pelas partes interessadas.

Estão incluídos neste âmbito os fluxos de informação crítica, que incluem a captação de dados, respetivo processamento, armazenamento, partilha com partes interessadas, assim como a respetiva destruição em modo seguro.

3. PARTES INTERESSADAS

Entende-se como partes interessadas todos 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 do Alto Minho; 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.

4. COMPROMISSOS PARA A SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

O Município de Ponte de Lima acompanha os avanços legislativos nacionais e europeus intentando, através da presente Política, garantir o compromisso de proteção de informação classificada como crítica para os seus serviços essenciais, incluindo dados pessoais dos titulares identificados como partes interessadas, comprometendo-se a identificar e tratar o risco de segurança de que esta seja, de modo acidental ou ilícito, perdida, destruída, alterada indevidamente ou acedida por quem não autorizado.

A presente Política define os compromissos assumidos pelo Município para a Segurança da Informação e Cibersegurança, que consistem nas seguintes garantias:

- **Confidencialidade** – Assegurar que apenas os utilizadores, internos ou externos, formalmente autorizados têm acesso à informação;
- **Privacidade** – Assegurar que os dados pessoais dos respetivos titulares, classificados como informação confidencial, apenas são recolhidos, processados e armazenados de acordo com fundamento legal válido nos termos dos princípios do quadro legal vigente;
- **Integridade** – Assegurar a proteção da informação contra a modificação e/ou destruição não autorizada, salvaguardando a respetiva veracidade e autenticidade;
- **Disponibilidade** – Assegurar que o acesso à informação é realizado sempre que necessário para a realização de uma atividade, preservando a confidencialidade, privacidade e integridade;
- **Não Repúdio** – Assegurar que todos os utilizadores, quando na condição de emissores de informação ou quando partilham dados pessoais com destinatários autorizados, serão sempre identificados física e digitalmente com valor probatório legal.
- **Cibersegurança –** Assegurar a proteção dos compromissos acima identificados quando os serviços essenciais e os ativos/recursos associados estão expostos ao Ciberespaço e a possíveis Ciberataques

5. PLANO DE SEGURANÇA

O Plano de Segurança tem como missão a definição, implementação, manutenção e melhoria contínua de um conjunto de regras, práticas, controlos de segurança, ações de monitorização e auditoria que permitam garantir a execução dos compromissos assumidos pelo Município no âmbito de proteção para a Segurança da Informação.

Para atingir com eficácia os compromissos e objetivos assumidos na presente política serão adotados os seguintes mecanismos de operacionalização:

- Definição, aprovação e divulgação de políticas temáticas complementares para a gestão da Segurança da Informação;
- Promoção de ações de sensibilização, formação e treino dos trabalhadores;

- Análise e gestão dos riscos identificados, incluindo o(s) respetivo(s) plano(s) de tratamento do risco e o respetivo risco residual;
- Identificação e operacionalização de controlos de segurança para tratamento do risco;
- Gestão dos incidentes de segurança de informação e respetivas respostas para garantia da continuidade do sistema de informação nas atividades definidas no âmbito de proteção;
- Realização de auditorias internas para identificação de oportunidades de melhoria;
- Revisão do Plano de Segurança e respetivas métricas de eficácia.

6. GESTÃO DO RISCO

Por se considerar uma ferramenta imprescindível no cumprimento dos objetivos do Plano de Segurança e da execução dos compromissos de segurança da presente política, serão feitas, periodicamente, análises de risco com o objetivo de serem adotadas as medidas de tratamento adequadas e proporcionais aos níveis dos riscos identificados.

Os controlos de segurança a implementar serão selecionados em função dos resultados dessa análise, com objetivo de assegurar a redução do risco, com eficácia, e a minimização do risco residual.

7. INTEGRAÇÃO COM A GESTÃO DA PRIVACIDADE DE DADOS PESSOAIS

Através da definição da garantia de privacidade, como um dos compromissos da segurança da informação, o Município executa a implementação integrada de controlos de segurança que assegurem as medidas de tratamento do risco adequadas para cumprimento dos requisitos do Regulamento Geral sobre a Proteção de Dados, e legislação conexa, e na estrita conformidade para com a Política de Privacidade e Tratamento de Dados Pessoais do Município.

8. CIBERSEGURANÇA

A informação crítica para os serviços essenciais, assim como os dados pessoais utilizados pelos processos internos do Município, em função da definição do âmbito de proteção, serão protegidos adequadamente contra os ataques e ameaças externos ou internos que sejam realizados através de mecanismos ou métodos que coloquem em causa a Cibersegurança do Município e de todos quantos com o mesmo interagem.

Para este efeito, entende-se como Cibersegurança a garantia de que os compromissos de segurança desta política são assegurados, mesmo havendo lugar a possíveis exposições ao Ciberespaço e, como consequência, os ativos expostos poderem ser alvo de Ciberataques.

O Município cumprirá os requisitos e práticas determinados pelo quadro legal do ***Regime Jurídico da Segurança do Ciberespaço,*** e procederá à adoção de boas práticas, medidas e controlos de segurança adequados, constantes no **QNRCS** - ***Quadro Nacional de Referência para a Cibersegurança***, normativos de referência e recomendações da ***European Union Agency for Cybersecurity*** **(ENISA)**, bem como implementará os procedimentos de gestão de incidentes necessários para identificar e tratar ataques ou ameaças.

Complementarmente, o Município implementará medidas de prevenção e proteção adequadas e proporcionais para assegurar o cumprimento das obrigações assumidas na presente política.

9. GESTÃO DE INCIDENTES

Um incidente de segurança ocorre quando um dos compromissos de segurança incluídos na presente política é violado, ou seja, não é possível ser mantido e demonstrado.

O Município compromete-se a implementar um procedimento de gestão de incidentes, gerido pelo Responsável de Segurança, tendo como objetivo a contenção do possível impacto de um ataque interno ou externo, e a retoma do funcionamento dos seus serviços essenciais o mais rapidamente possível.

Ciente da sua responsabilidade para com as partes interessadas, este procedimento inclui atividades de comunicação que permitem informar adequadamente do estado de evolução e tratamento de qualquer incidente de segurança.

Neste contexto, destaca-se a integração do procedimento de notificação de incidentes de Cibersegurança à entidade nacional designada, Centro Nacional de Cibersegurança.

10. FUNÇÕES E RESPONSABILIDADES

Os intervenientes com funções e responsabilidades em relação á gestão e aplicação desta política são os seguintes:

1. Executivo

O Executivo assegura que a presente política e os objetivos de segurança estão estabelecidos e são adequados para com a orientação estratégica do Município de Ponte de Lima, assim como a integração nos processos organizativos dos requisitos de segurança da informação, bem como a alocação dos recursos necessários para gestão eficaz do Plano de Segurança.

O Executivo aprova, delibera, no âmbito das duas competências, as medidas necessárias para a implementação com eficácia do Plano de Segurança do Município.

2. Responsável de Segurança

O Responsável de Segurança é nomeado pelo Presidente da Câmara Municipal para assumir, nomeadamente, as seguintes funções:

- Garantir a definição de tarefas de implementação, manutenção e operação da estratégia da Segurança da Informação e Cibersegurança do Município;
- Assegurar a conformidade com a legislação e regulamentação aplicável, incluindo Regime Jurídico da Segurança do Ciberespaço e quadro legal vigente atinente à proteção de dados;
- Ter conhecimento e garantir a implementação de boas práticas de Segurança da Informação e Cibersegurança;
- Supervisionar e aprovar a avaliação periódica dos riscos de segurança e respetivos tratamentos;

- Promover a elaboração de planos de formação/sensibilização/consciencialização relativos à segurança da informação a implementar junto dos trabalhadores do Municipio;
- Acompanhar e avaliar a gestão de incidentes de segurança e respostas em continuidade de serviços;
- Supervisionar a equipa responsável pela realização de auditorias internas necessárias.

3. Pontos de Contacto Permanente

O Presidente da Câmara é responsável pela designação de um número considerado suficiente, de Ponto de Contacto Permanente.

Estes recursos assumem as seguintes funções:

- Articular com outras entidades a eficácia da resposta a incidentes de segurança com impacto nas atividades do Município, sob supervisão do Responsável de Segurança;
- Proceder à operacionalização dos procedimentos atinentes ao Plano de Segurança do Município;
- Diligenciar a obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto relevante ou substancial submetidas pelo Município ou por outra entidade cujo sistema de informação possa ter algum tipo de impacto nas atividades do Município, incluindo instruções técnicas emitidas pelo Centro Nacional de Cibersegurança no âmbito das funções deste;
- Obtenção e atualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial;
- Promover a partilha de informação quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da segurança do ciberespaço, bem como de planos no âmbito do planeamento civil de emergência do ciberespaço ou dos planos de segurança das infraestruturas críticas nacionais ou europeias com impacto no sistema de informação do Município;
- A operacionalização dos procedimentos fixados no âmbito de eventuais planos de emergência de proteção civil quando estes tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência do ciberespaço;

4. Utilizadores do Sistema de Informação

Todos os utilizadores autorizados do Sistema de Informação Municipal serão sensibilizados, através de ações incluídas em plano de formação interno, por forma a desempenhar as funções inerentes à sua categoria profissional em conformidade com a missão, objetivos e obrigações previstas na presente política.

Após a divulgação e publicação desta Política, ficam os utilizadores de recursos do Sistema de Informação obrigados a:

- Frequentar as ações de formação incluídas no plano de formação em vigor, seja aquando da sua integração no Município, aquando de mudança de funções ou de acordo com a definição de periodicidade de repetição de cada ação de formação;

- Proteger os ativos de informação a seu cargo;
- Colaborar na gestão do respetivo risco dos recursos atribuídos;
- Assegurar que os recursos que são atribuídos são apenas usados para fins profissionais;
- Participar qualquer evento que possa colocar em causa a segurança da informação;
- Atender e seguir as comunicações/informações que são transmitidas pelo Município no âmbito da Segurança da Informação e Segurança do Ciberespaço;
- Cumprir e fazer cumprir a presente política.

No caso de desrespeito pelo disposto na presente política, o Município irá executar os procedimentos necessários para que o infrator, nos termos da responsabilidade civil, criminal, contraordenacional e/ou disciplinar, seja responsabilizado pelos seus atos.

11. PLANO DE SENSIBILIZAÇÃO, FORMAÇÃO E TREINO

O Município assegura a operacionalização de um plano periódico de sensibilização, formação e treino dos utilizadores, que inclui comunicação de boas práticas, ações de formação "*online*" e presenciais, assim como testes dos procedimentos de resposta a incidentes para treino e prontidão.

A eficácia deste plano é realizada através de um conjunto de iniciativas que visam a garantia de capacitação e prontidão dos utilizadores para a Segurança da Informação, a Cibersegurança, assim como a Ciberhigine pessoal prevista no Plano de Segurança.

12. MANUTENÇÃO, MELHORIA CONTÍNUA E REVISÃO

Todas as políticas, procedimentos e demais documentos de suporte ao Plano de Segurança, serão revistos e atualizados sempre que existirem alterações de contexto e estratégia do Município, alterações da lista de partes interessadas e respetivos requisitos, ou ainda devido à realização de alterações organizativas relevantes nos seus processos decorrentes do exercício das competências atribuídas.

O Responsável de Segurança compromete-se, ainda, que esta revisão e atualização será realizada, pelo menos, anualmente.

13. DIVULGAÇÃO E PUBLICAÇÃO

Tendo em conta a classificação desta política, este documento será divulgado em formato PDF não editável a todas as partes interessadas através dos canais de comunicação digitais do Município.

14. REGISTO DE REVISÃO

VERSÃO	MOTIVO DA REVISÃO	ELABORADO POR	APROVADO POR	DATA APROVAÇÃO
0.1	Criação e redação preliminar	Serviço de Informática	Responsável de Segurança	14/12/2023
1.0	Aprovação	Serviço de Informática	Câmara Municipal	26/12/2023