



Município de Paredes de Coura
Regulamento Interno de Segurança do
Sistema de Informação do Município

2025

Aprovado na reunião da Câmara Municipal de 20-06-2025



Índice

CAPÍTULO I – DISPOSIÇÕES GERAIS	3
Artigo 1.º - Objeto do Regulamento	3
Artigo 2.º - Âmbito do Regulamento	3
Artigo 3.º - Definições	3
CAPÍTULO II – GESTÃO DO ACESSO À INFORMAÇÃO	4
Artigo 4.º - Princípios gerais do acesso à informação	4
Artigo 5.º - Responsabilidades – Município	4
Artigo 6.º - Responsabilidades – Dirigentes	5
Artigo 7.º - Responsabilidades – Setor de Informática	5
Artigo 8.º - Direitos da pessoa autorizada	6
CAPÍTULO III – USO ACEITÁVEL DE ATIVOS	6
Artigo 9.º - Gestão de Acessos	6
Artigo 10.º - Uso do Correio Eletrónico	6
Artigo 11.º - Gestão da Informação	7
Artigo 12.º - Rede e Equipamentos Informáticos	8
Artigo 13.º - Acesso à Internet	9
Artigo 14.º - Espaço de Trabalho e Documentos Físicos	9
Artigo 15.º - Acesso remoto e teletrabalho	10
Artigo 16.º - Dispositivos móveis	10
CAPÍTULO IV – SEGURANÇA E MONITORIZAÇÃO	11
Artigo 17.º - Segurança e Monitorização	11
Artigo 18.º - Monitorização e criação de registos	11
Artigo 19.º - Apoio técnico - Solicitações ao Setor de Informática - HelpDesk/ServiceDesk	11
Artigo 20.º - Notificação de incidentes	11
Artigo 21.º - Gestão de Incidentes	12
CAPÍTULO V – AUDITORIA E REGIME DISCIPLINAR	12
Artigo 22.º - Auditoria	12
Artigo 23.º - Regime disciplinar	12
CAPÍTULO VI – DISPOSIÇÕES FINAIS	12
Artigo 24.º - Procedimento, comunicação e localização do Regulamento	12
Artigo 25.º - Aprovação do Regulamento	12
Artigo 26.º - Revisão do presente regulamento	12
Artigo 27.º - Dúvidas e omissões	12
Artigo 28.º - Entrada em vigor	12



MUNICÍPIO DE PAREDES DE COURA

Câmara Municipal



Regulamento de Segurança do Sistema de Informação do Município de Paredes de Coura

Preâmbulo

O Município de Paredes de Coura reconhece o valor estratégico que a informação desempenha para a prossecução da sua missão enquanto autarquia local. Assim sendo, pretende com a redação do presente Regulamento da Segurança do Sistema de Informação, estabelecer modos de proceder e orientações para toda a estrutura organizacional em estrita conformidade com legislação e normativos em vigor em matéria de proteção de dados pessoais, segurança de redes, sistemas de informação e Cibersegurança, e criminalidade informática, designadamente, Regulamento (UE) 2016/679 de 27 de abril, Regulamento Geral sobre a Proteção de Dados, RGPD, Lei 58/2019 de 8 de agosto, execução nacional do RGPD, Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de Dezembro de 2022, Lei n.º 46/2018 de 13 de agosto – Regime Jurídico da Segurança do Ciberespaço, Decreto-Lei n.º 65/2021 de 30 de julho e Lei n.º 109/2009 de 15 de Setembro – Lei do Cibercrime.



CAPÍTULO I – DISPOSIÇÕES GERAIS

Artigo 1.º - Objeto do Regulamento

Através do presente Regulamento, o Município de Paredes de Coura visa definir um conjunto de direitos e deveres para os utilizadores do sistema de informação, abrangendo todas as suas componentes, digitais e físicas, por forma a promover a segurança da informação garantindo a sua confidencialidade, integridade, disponibilidade e privacidade dos dados pessoais. Pretendendo evitar que a informação seja perdida, destruída, alterada indevidamente ou acedida por quem não autorizado.

Artigo 2.º - Âmbito do Regulamento

1. O Regulamento de Segurança do Sistema de Informação aplica-se a todas as pessoas autorizadas a aceder e a tratar informação do Município de Paredes de Coura, com o objetivo de orientar e regular as suas ações no domínio da segurança dos sistemas de informação;
2. O presente Regulamento aplica-se a toda a informação mantida e tratada sob a responsabilidade do Município de Paredes de Coura, independentemente do seu suporte de registo: eletrónico, físico, incluindo papel, audiovisual ou outro.

Artigo 3.º - Definições

1. **Pessoa autorizada** - Consideram-se pessoas autorizadas para efeitos do presente documento, as/os funcionárias/os do município, as/os contratada/o(s), as/os eleitos locais, as/os colaboradora/e(s) em regime de prestação de serviços e outros agentes que utilizem recursos da autarquia ou pessoais para aceder, armazenar, fazer *backup* ou realocar qualquer informação da autarquia;
2. **Regulamento da Segurança do Sistema de Informação** – Documento que orienta ou regula as ações das pessoas ou sistemas no domínio da segurança do sistema de informação;
3. **Sistema de Informação** – Conjunto integrado de componentes para recolha, armazenamento e processamento de dados, automatizado ou não, que suporte o fornecimento de informações e o conhecimento a uma organização;
4. **Confidencialidade** – propriedade de que a informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados;
5. **Integridade** – propriedade relativa à exatidão e completude da informação e dos seus métodos de processamento;
6. **Disponibilidade** – propriedade de que a informação está acessível e utilizável quando requerido por uma entidade autorizada;
7. **Não repúdio** – garantia que todos os utilizadores quando na condição de emissores de informação ou quando partilham dados com destinatários autorizados, serão sempre identificados, física e digitalmente, com valor probatório legal;
8. **Privacidade** – característica de segurança de um sistema de informação que permite definir quais os dados que podem, ou não, ser acedidos por terceiro;
9. **Segurança de Sistemas de Informação** – Enquadramento organizacional de cultura, políticas, estruturas organizacionais e ambiente operacional utilizado para assegurar a integridade, disponibilidade e confidencialidade da informação de uma organização;
10. **Segurança das redes e dos sistemas de informação** - capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, a integridade, a



disponibilidade, a autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles;

11. **Sistema informático** – qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;
12. **Dados informáticos** – qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;
13. **Ativo** – qualquer coisa que tenha valor para a organização;
14. **Ativo Essencial** – componente do sistema de informação, hardware, software ou aplicação que suporte um serviço essencial prestado pelo Município;
15. **Dono do Ativo** – recurso interno responsável por um ativo;
16. **Incidente** – um evento com um efeito adverso na segurança das redes e dos sistemas de informação;
17. **Phishing** – procedimento que recorre ao envio de mensagens que usam técnicas de engenharia social de modo que o alvo seja ludibriado 'mordendo o isco', entregando informação confidencial;
18. **Tratamento de incidentes** – todos os procedimentos de apoio à deteção, análise, contenção e resposta a um incidente;
19. **Rede privada virtual (VPN)** – Rede virtual de comunicação privada que utiliza uma infraestrutura pública de telecomunicações para transmitir dados que são protegidos devido à utilização de técnicas de cifragem ou de encapsulação;
20. **Dispositivo móvel** – computador portátil, tablet, smartphone ou similar, propriedade do Município, ou não, que seja utilizado para acesso, processamento e armazenamento de informação detida pelo Município;
21. **Metadados** – Descrição ou conjunto de características de um dado ou de um item, especialmente em relação a informação processada por computador, como, por exemplo, o tamanho ou o tipo de um ficheiro, ou ainda a data da última alteração.

CAPÍTULO II – GESTÃO DO ACESSO À INFORMAÇÃO

Artigo 4º - Princípios gerais do acesso à informação

O Município implementa controlos de acesso físicos e lógicos que restringem o acesso à informação tendo por base a avaliação da:

- **Necessidade de Conhecer:** o acesso à informação está restrito a quem necessita de a conhecer para a prossecução das suas competências;
- **Necessidade de Uso:** o acesso a espaços físicos que contenham dados, quer em formato físico que em formato digital, apenas deve ser concedido caso seja necessário para o desempenho das funções atribuídas.

Artigo 5º - Responsabilidades – Município

1. O Município define e mantém um processo formal de disponibilização de contas de acesso às várias componentes do sistema de informação para atribuir, alterar ou revogar os direitos de acesso:



- a. O acesso a componentes do sistema de informação, dispositivos, aplicações, sistemas ou similares, é feito mediante um processo com autenticação auditável. Este, pode recorrer ao uso de credenciais de acesso, como nome de utilizador e palavra-passe ou equivalente, atribuídas ao trabalhador/Unidade Organizacional, com base em proposta do dirigente competente;
- b. A atribuição de direitos de acesso e privilégio às componentes do sistema de informação, é feita mediante a definição de perfis com privilégios mínimos e diferenciados, seguindo o princípio da necessidade de conhecer e aceder à informação;
- c. O Município aprova e comunica perante as partes interessadas, definidas em sede de Plano de Segurança, uma Política de Segurança da Informação e uma Política de Privacidade;
- d. O Município, através de órgão competente, aprova e autoriza o exercício das funções profissionais em formato de teletrabalho e trabalho remoto.

Artigo 6º - Responsabilidades – Dirigentes

1. As necessidades de acesso às componentes do sistema de informação e correspondente perfil de permissões de cada pessoa autorizada são definidas pelo superior hierárquico que, em momento de admissão ou de alteração de funções, assume responsabilidades de direção, devendo o mesmo:
 - a. Notificar o Setor de Informática:
 - Quanto às necessidades de acesso ao sistema de informação do Município através de procedimento que crie registo auditável;
 - Quanto à autorização prestada a determinado trabalhador para acesso remoto à infraestrutura digital do município.
 - b. Notificar o Setor de Recursos Humanos, quanto a qualquer alteração nas funções a desempenhar por pessoa autorizada que implique alteração no acesso à informação e aos respetivos sistemas.

Artigo 7º - Responsabilidades – Setor de Informática

1. O Setor de Informática é a unidade organizacional responsável pela gestão do Sistema de Informação, de caráter digital, onde se inclui a gestão de identidades e controlo de acessos, o conjunto de acessos privilegiados e de administração de sistemas e redes. No âmbito do objeto deste Regulamento, o Setor de Informática:
 - a. Gere os acessos externos autorizados ao sistema de informação do Município através de recursos que suportem ligações seguras;
 - b. É responsável pela definição, manutenção e monitorização de procedimentos de cópia de backup apropriados que salvaguardem os ativos selecionados da infraestrutura digital, de forma a garantir a sua integridade e disponibilidade;
 - c. É a única unidade orgânica autorizada a instalar, mover e proceder ao abate de qualquer equipamento integrado em sistema digital do Município;
 - d. Implementa, sempre que tecnicamente possível, controlos de cifra para proteção de dados em equipamentos portáteis;
 - e. Analisa e define requisitos de segurança a incluir em equipamentos do que processem informação, incluindo equipamentos do tipo Dispositivo Móvel;
 - f. Mantém um registo de todo o software autorizado e executa a correspondente gestão de licenças e termos de uso;



- g. É responsável pela gestão da componente de administração das caixas de correio eletrónico do serviço do Município, estando essa gestão restrita à criação, suspensão, eliminação e gestão de atributos gerais do serviço de correio eletrónico.

Artigo 8.º - Direitos da pessoa autorizada

A pessoa autorizada tem direito à liberdade e privacidade no âmbito do tratamento informático dos seus dados pessoais e no âmbito do trabalho técnico da sua responsabilidade e autoria.

CAPÍTULO III – USO ACEITÁVEL DE ATIVOS

Artigo 9.º - Gestão de Acessos

1. A pessoa autorizada deve:
 - a. Respeitar boas práticas para a escolha ou composição de palavras-passe, nomeadamente: não usar como palavras-passe palavras únicas do dicionário, datas, ou outras que lhe sejam facilmente associáveis;
 - b. Manter as palavras-passe confidenciais, guardar as palavras-passe em software dedicado ou ficheiros cifrados com acesso restrito;
 - c. Mudar as palavras-passe regularmente, seguindo os procedimentos comunicados formalmente pelo Setor de Informática;
 - d. Alterar imediatamente a palavra-passe e contactar o Setor de Informática, em caso de suspeita de compromisso de conta;
 - e. Bloquear/sair da sessão, sempre que se ausentar do seu local de trabalho evitando, assim, o acesso não autorizado. O utilizador que estiver autenticado é responsável pelas ações executadas a partir do computador e/ou aplicações;
 - f. Utilizar a autenticação multifator em todas os sistemas que ofereçam essa possibilidade.
2. A pessoa autorizada não deve:
 - a. Reutilizar palavras-passe em uso em sistemas do Município em contextos de uso pessoal;
 - b. Partilhar as suas credenciais de acesso com terceiros. Caso tal ocorra a pessoa autorizada é considerada a única responsável pelo uso das mesmas;
 - c. Manter as palavras-passe escritas em papéis ou em locais visíveis;
 - d. Associar contas de utilizador de uso pessoal (ex. Gmail ou similar) a sistemas do Município, que possibilitem por exemplo, gravar palavras-passe de forma automática;
 - e. Usar recursos informáticos que não lhe estejam diretamente atribuídos, ou aos quais não deva aceder, no decurso do exercício de competências.

Artigo 10.º - Uso do Correio Eletrónico

1. A pessoa autorizada deve:
 - a. Usar o sistema de correio eletrónico institucional seguindo os princípios gerais de Ética e Conduta aplicáveis aos trabalhadores da Administração Pública;
 - b. Analisar os e-mails recebidos a fim de detetar sinais de *phishing*/fraude antes de os utilizar. Alguns sinais de alerta podem ser:



- Remetente ou domínio de e-mail desconhecido/suspeito;
 - Pedido ou assunto inesperado;
 - Sentido de urgência;
 - Erros ortográficos;
 - Tratamento como “Caro cliente”;
 - URL longos ou complexos em hiperligações incluídas no corpo do e-mail.
- c. Verificar, em cada envio, se o destinatário está corretamente preenchido;
- d. Comunicar ao Encarregado de Proteção de Dados qualquer envio de e-mail para o destinatário errado, caso este contenha dados pessoais.
2. A pessoa autorizada não deve:
- a. Abrir anexos de e-mail ou clicar em ligações à Internet (URL) em mensagens de e-mail suspeitas ou provenientes de um remetente desconhecido/suspeito;
 - b. Abrir anexos de e-mail ou clicar em ligações à Internet (URL) em mensagens de e-mail provenientes de um remetente conhecido, mas com um pedido não habitual;
 - c. Usar o endereço de e-mail institucional para registo em redes sociais ou plataformas e sítios web similares não diretamente relacionados com o desempenho de funções profissionais e institucionais;
 - d. Reencaminhar o e-mail institucional para contas de e-mail pessoais, ou usar contas de e-mail pessoais para fins profissionais;
 - e. Usar o e-mail institucional para fins não compatíveis com o exercício da atividade do Município, nomeadamente para atividades comerciais privadas;
 - f. Usar o e-mail institucional para criar ou distribuir mensagens disruptivas ou ofensivas, incluindo comentários ofensivos sobre raça, sexo, deficiências, orientação sexual, pornografia, crenças e práticas religiosas, crenças políticas ou origem nacional;
 - g. Reencaminhar mensagens de e-mail de acesso restrito, que contenham informações confidenciais, para destinatários não expressamente autorizados a aceder à informação.

Artigo 11.º - Gestão da Informação

1. A pessoa autorizada deve:
- a. Manter total confidencialidade sobre informação que não seja de natureza pública, sobre a qual tome conhecimento no decurso do desempenho da atividade profissional ao serviço do Município;
 - b. Comunicar imediatamente, ao Setor de Informática, o roubo, perda ou dano de qualquer ativo eletrónico do Município;
 - c. Usar os repositórios digitais (diretorias) atribuídas a cada Unidade Organizacional e/ou Utilizador. Apenas sobre os mesmos é garantida a aplicação do procedimento de backup em vigor – O Setor de Informática não se responsabiliza pela perda de dados arquivados fora das diretorias atribuídas;
 - d. Fazer a manutenção periódica do diretório pessoal, evitando o acumular de informação não necessária no servidor de rede;



- e. Garantir que eventuais documentos a publicar no site institucional, ou a enviar para terceiros, não contenham metadados com dados pessoais ou outra informação não relevante para a finalidade de partilha ou publicação.
2. A pessoa autorizada não deve:
 - a. Divulgar informação confidencial ou respeitante à vida privada de outros trabalhadores, excetuando-se todas as situações decorrentes das atividades do Município;
 - b. Transferir qualquer informação confidencial para um computador ou dispositivo móvel que não seja do Município;
 - c. Enviar dados do Município em suporte digital para Clouds públicas, ou plataformas de uso similar que não sejam disponibilizadas pelo Município – inclui-se neste âmbito o uso de soluções tipo WhatsApp para registo e partilha de cópias de documentos do Município acedidos em contexto profissional;
 - d. Guardar nos sistemas do Município ficheiros pessoais, fotografias, vídeos, músicas e programas informáticos que não sejam para uso em contexto profissional;
 - e. Carregar ficheiros, nomeadamente fotografias, com resoluções elevadas. A ter de o fazer, dever-se-á restringir aos ficheiros efetivamente necessários para suporte das tarefas do serviço;
 - f. Abordar informações de carácter institucional ou profissional em locais públicos ou privados sem garantia de reserva de privacidade.

Artigo 12.º - Rede e Equipamentos Informáticos

1. A pessoa autorizada deve:
 - a. Fazer um uso adequado dos recursos disponibilizados pelo Município, nomeadamente de rede, por forma a não consumir recursos desproporcionais e impactar o uso dos outros utilizadores;
 - b. Terminar a sessão/encerrar em aplicações, serviços ou no final de uso;
 - c. Desligar todos os equipamentos utilizados, incluindo computadores, sempre que ocorrer uma pausa prolongada no uso e, obrigatoriamente, no final do dia de trabalho;
 - d. Solicitar ao Setor de Informática qualquer necessidade de realocação de dispositivos;
 - e. Informar o Setor de Informática caso se depare com algum comportamento inesperado ou anormal, no dispositivo, ou na rede ou na Internet.
2. A pessoa autorizada não deve:
 - a. Interferir com dados, programas ou sistemas, nem intercetar informação de outra pessoa autorizada ou do Município;
 - b. Proceder à ligação de novos equipamentos à rede interna do Município sem prévia solicitação ao Setor de Informática;
 - c. Utilizar recursos informáticos do Município para fins comerciais, ou pessoais, não relacionados com o Município;
 - d. Instalar aplicações, software executável ou similar, nem alterar a configuração das aplicações ou sistemas instalados.



Artigo 13.º - Acesso à Internet

1. A pessoa autorizada deve:
 - a. Usar apenas software autorizado pelo Município;
 - b. Usar soluções de cloud pública quando autorizado previamente pelo Setor de Informática;
 - c. Inserir informação apenas em sites e plataformas de entidades públicas e privadas com quem o Município mantenha relações contratuais ou institucionais;
 - d. Consultar o Setor de Informática sempre que um site ou plataforma apresente um comportamento não esperado ou pedidos anormais.
2. A pessoa autorizada não deve:
 - a. Aceder a sites ou aplicações com conteúdo inapropriado ou ofensivo não condizentes com o desempenho das funções profissionais no Município;
 - b. Recorrer ao uso de aplicações que tem como objetivo contornar as restrições de acesso definidas pelo Município;
 - c. Aceder a sites ou aplicações que consumam recursos de rede excessivos tais como plataformas de *streaming* de média e jogos online;
 - d. Transferir material protegido por direitos de autor sem a devida autorização, estando o eventual uso sujeito às penalidades criminais e cíveis que daí possam advir;
 - e. Introduzir informação do Município de carácter sigiloso em soluções de inteligência artificial generativa.

Artigo 14.º - Espaço de Trabalho e Documentos Físicos

1. A pessoa autorizada deve:
 - a. Assegurar que os documentos em formato físico são mantidos de forma a prevenir acesso não autorizado, em especial em zonas de acesso público;
 - b. Arquivar documentos em suporte físico em arquivo fechado/acesso restrito, em caso de ausência prolongada ou no final do dia;
 - c. Dispor os ecrãs de computador de forma a prevenir a sua visualização por quem não autorizado;
 - d. Fechar armários, gavetas ou similares que contenham informação quando não em uso e em horário não laboral;
 - e. Tomar medidas adequadas para preservar a segurança de documentos em contexto de transporte fora dos espaços físicos do Município, nomeadamente quanto a acesso não autorizado;
 - f. Usar código de utilizador atribuído para ativação do sistema de impressão em uso no Município. O utilizador que ceda o código a terceiros é responsável pelo seu uso indevido incluindo acesso não autorizado a documentos;
 - g. Recorrer a meios adequados para a destruição de documentos em formato físico, nomeadamente destruidoras de papel.
2. A pessoa autorizada não deve:
 - a. Deixar documentos em locais de acesso público ou de passagem de forma que os mesmos fiquem ao alcance físico ou visíveis por quem não autorizado;



- b. Fazer registo fotográfico, vídeo ou similar de documentos em formato físico ou outro suporte de dados, quando não autorizado;
- c. Usar sistemas de impressão e digitalização sem autorização.

Artigo 15.º - Acesso remoto e teletrabalho

1. A pessoa autorizada deve:
 - a. Aceder remotamente ao sistema de informação do município unicamente através de soluções disponibilizadas e geridas pelo Setor de Informática;
 - b. Apenas usar equipamentos disponibilizados pelo Município para suporte de acessos remotos, através de VPN (Rede Privada Virtual);
 - c. Garantir que o trabalho realizado é feito em documentos armazenados na infraestrutura do Município ou que caso tal não seja possível, os documentos devem ser transferidos para a infraestrutura do Município.
2. A pessoa autorizada não deve:
 - a. Disponibilizar a terceiros, incluindo familiares, equipamentos do Município em uso para trabalho remoto;
 - b. Recorrer ao uso de redes públicas inseguras para suporte de acesso remoto aos sistemas informáticos do município;
 - c. Tentar instalar qualquer software ou outras aplicações, em dispositivos móveis, não licenciadas ao Município de Paredes de Coura.

Artigo 16.º - Dispositivos móveis

Por dispositivo móvel entende-se computador portátil, tablet, smartphone ou similar, propriedade do Município, ou não, que seja utilizado para acesso, processamento e armazenamento de informação detida pelo Município.

1. A pessoa autorizada deve:
 - a. Submeter qualquer dispositivo móvel ao Setor de Informática, antes de iniciar a sua utilização, para a ativação das configurações de segurança;
 - b. Ativar palavra-passe, PIN ou equivalente, para autenticação e acesso ao dispositivo móvel;
 - c. Ativar as ligações Wifi e Bluetooth, apenas e só, quando o uso das mesmas é estritamente necessário;
 - d. Ativar o bloqueio automático em caso de inatividade;
 - e. Entregar o dispositivo ao Setor de Informática no fim de uso para remoção segura de dados e configurações;
 - f. Notificar o Setor de Informática em caso de perda ao roubo de dispositivo móvel do Município ou com informação do Município;
 - g. Ativar serviços ou aplicações que acedam a informação do Município em dispositivos pessoais, caso tal decorra de conveniência de serviço justificada e apenas após validação pelo Setor de Informática quanto à existência de garantias mínimas de segurança.
2. A pessoa autorizada não deve:



- a. Transmitir as suas credenciais de acesso, e outros métodos de autenticação, a terceiros, incluindo aos membros da família e a outras pessoas autorizadas do Município;
- b. Ativar serviços ou aplicações que acedam a informação do Município em dispositivos pessoais;
- c. Transferir documentos do Município, por exemplo através de descarga do email, para o dispositivo móvel, pessoal ou de uso profissional;
- d. Deixar o dispositivo móvel em veículos automóveis sem vigilância;
- e. Ligar-se a redes wifi públicas que não apresentem garantias de segurança adequadas.

CAPÍTULO IV – SEGURANÇA E MONITORIZAÇÃO

Artigo 17.º - Segurança e Monitorização

1. Regime Jurídico da Segurança no Ciberespaço:
 - a. O Município deve garantir a disponibilização de recursos adequados ao cumprimento das obrigações legais decorrentes do Regime Jurídico da Segurança no Ciberespaço;
 - b. O Município define e mantém atualizado um Plano de Segurança que compreenda as principais tarefas de gestão da segurança da informação. Este integra uma Política de Segurança da Informação;
 - c. O Município deve designar Responsável pela Segurança que assuma a gestão do conjunto das medidas adotadas em matéria de segurança de redes e sistemas e de notificação de incidentes;
 - d. O Município deve designar pontos de contactos permanente com o Centro Nacional de Cibersegurança em número suficiente para assegurar as obrigações decorrentes do quadro legal.

Artigo 18.º - Monitorização e criação de registos

1. O Município deve definir e implementar, na sequência da identificação de necessidades que decorram da avaliação de risco, um conjunto de controlos técnicos que promovam a segurança de redes e sistemas, incluindo:
 - a. O uso de ferramentas automatizadas de inspeção de tráfego e deteção de intrusões, com vista à deteção e bloqueio de tráfego potencialmente malicioso, assim como de tentativas de acesso não autorizadas;
 - b. A recolha e armazenamento seguro de registos gerados pelos sistemas informáticos, para cumprimento de obrigações legais e suporte de eventuais procedimentos de análise forense.

Artigo 19.º - Apoio técnico - Solicitações ao Setor de Informática - HelpDesk/ServiceDesk

O Setor de Informática atuará de forma autónoma ou, de forma articulada com fornecedores externos, para ultrapassar quaisquer condições que se considerem anómalas na utilização dos sistemas informáticos, criando um registo do pedido.

Artigo 20.º - Notificação de incidentes

1. A pessoa utilizadora tem o dever de comunicar superiormente qualquer evidencia de tentativa e/ou acesso não autorizado ou qualquer outro uso indevido de recursos digitais ou físicos do sistema de informação;
2. O testemunho direto ou tomada de conhecimento de forma indireta de incidentes relacionados com a segurança ou uso abusivo de recursos, incluindo o desrespeito por este regulamento, deve ser comunicado ao superior hierárquico ou ao Setor de Informática.



Artigo 21.º - Gestão de Incidentes

1. Os incidentes de segurança relacionados com a componente digital do sistema de informação deverão ser comunicados ao Setor de Informática competindo-lhe diligenciar pela mitigação do incidente, pelo registo de evidências e subseqüente comunicação ao responsável pela segurança;
2. Os incidentes de segurança relacionados com a componente física do sistema de informação deverão ser comunicados pelo dirigente que superintende o espaço físico onde ocorra o incidente ao Vereador do Pelouro e ao Responsável de Segurança.

CAPÍTULO V – AUDITORIA E REGIME DISCIPLINAR

Artigo 22.º - Auditoria

1. O cumprimento deste regulamento, no que respeita à componente de infraestrutura digital, incluindo a atividade realizada pela pessoa utilizadora nos equipamentos informáticos do Município poderá, em qualquer altura ser objeto de auditoria, pelo Setor de Informática, de forma a garantir o cumprimento das normas de utilização e de modo a assegurar a qualidade e o bom funcionamento da prestação dos serviços de tecnologias e informação e comunicação;
2. As auditorias são realizadas pelo Setor de Informática a pedido do responsável do pelouro ou do Responsável de Segurança designado.

Artigo 23.º - Regime disciplinar

O não cumprimento das normas do presente regulamento pode determinar a abertura dos competentes procedimentos disciplinares, nos termos da lei, sem prejuízo da responsabilidade criminal que vier a ser apurada nessa sede.

CAPÍTULO VI – DISPOSIÇÕES FINAIS

Artigo 24.º - Procedimento, comunicação e localização do Regulamento

O presente regulamento interno deverá ser publicitado nos termos da Lei, sendo o mesmo diploma disponibilizado na *intranet* e distribuído, via *e-mail*, para todas as pessoas utilizadoras.

Artigo 25.º - Aprovação do Regulamento

O presente Regulamento foi aprovado pela Câmara Municipal de Paredes de Coura no dia 18 de junho de 2025.

Artigo 26.º - Revisão do presente regulamento

O presente regulamento poderá ser objeto de alteração por iniciativa da Câmara Municipal.

Artigo 27.º - Dúvidas e omissões

As dúvidas e omissões do presente regulamento serão resolvidas por recurso à interpretação da legislação habilitante, com base em critérios de equidade, mediante decisão do Presidente da Câmara Municipal de Paredes de Coura.

Artigo 28.º - Entrada em vigor

O presente documento entra em **vigor 05 dias após** a deliberação de aprovação tomada pela Câmara Municipal.