Presente à reunião de câmara e
deliberado por unanimidade aprovar

reunião do dia 18/06/2026 - Ata n. 17

Regulamento de Segurança do Sistema de Informação do Município de Valpaços

INDICE

Regulamento de Segurança do Sistema de Informação do Município de Valpaços

Preâmbulo

O Município de Valpaços, no cumprimento das suas atribuições e visando salvaguardar a continuidade e fiabilidade dos serviços municipais, reconhece a importância da proteção da informação e das redes e sistemas de informação que suportam a sua atividade, incluindo os sistemas e processos associados à prestação de serviços essenciais à população, incluindo ao fornecimento de água potável, com impacto direto na confiança dos munícipes e no ecossistema local.

A crescente transformação digital e interligação da sociedade têm ampliado o contexto de ciberameaças e o impacto dos incidentes, exigindo respostas proporcionais e coordenadas, enquadradas no esforço legislativo europeu em matéria de cibersegurança, designadamente na Diretiva (UE) 2022/2555, transposta para a ordem jurídica interna pelo Regime Jurídico da Segurança do Ciberespaço aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro, e pela regulamentação complementar aplicável, na versão vigente.

Dando continuidade ao esforço já desenvolvido, o Município procede à revisão do Regulamento anteriormente em vigor, aprovando o presente Regulamento de Segurança do Sistema de Informação, com vista a garantir a confidencialidade, integridade e disponibilidade da informação, incluindo dados pessoais, e a definir e implementar medidas de cibersegurança adequadas ao contexto e ao risco, em alinhamento com o Quadro Nacional de Referência para a Cibersegurança (QNRCS), na versão vigente, e orientações aplicáveis da autoridade competente. Este Regulamento estabelece os direitos e deveres das pessoas autorizadas e as regras de utilização e proteção aplicáveis às componentes digitais e físicas do sistema de informação municipal.

CAPÍTULO I - DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto do Regulamento

1 — O presente Regulamento define as regras e práticas de segurança aplicáveis ao Sistema de Informação do Município de Valpaços, visando assegurar a confidencialidade, integridade e disponibilidade da informação, incluindo dados pessoais, bem como prevenir a ocorrência e mitigar o impacto de incidentes que possam comprometer o regular funcionamento da autarquia.

2 — O presente Regulamento estabelece, ainda, os princípios e regras de utilização dos recursos do Sistema de Informação, bem como as responsabilidades associadas, promovendo a adoção de medidas de cibersegurança proporcionais ao contexto do Município e ao risco, nos termos do quadro legal aplicável.

3 — O disposto no presente Regulamento é interpretado e aplicado em conformidade com a legislação e normativos aplicáveis em matéria de proteção de dados pessoais, criminalidade informática e cibersegurança, designadamente o Regulamento (UE) 2016/679 (RGPD), a Lei n.º 58/2019, a Lei n.º 109/2009 (Lei do Cibercrime) e o Regime Jurídico da Cibersegurança aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro, bem como a respetiva regulamentação complementar aplicável, na versão vigente.

4 — Para efeitos de implementação das medidas de cibersegurança, o Município atende aos referenciais nacionais aplicáveis, incluindo o Quadro Nacional de Referência para a Cibersegurança (QNRCS), na versão vigente, e demais orientações técnicas aplicáveis emitidas pela autoridade competente.

Artigo 2.º

Âmbito do Regulamento

1 — O presente Regulamento aplica-se a todas as pessoas autorizadas a aceder e a tratar informação do Município de Valpaços, independentemente de o acesso ou tratamento ocorrer em suporte físico ou digital, com o objetivo de orientar e regular as suas ações no domínio da segurança do Sistema de Informação.

2 — O presente Regulamento aplica-se a toda a informação mantida e tratada sob responsabilidade do Município de Valpaços, independentemente do seu suporte de registo, designadamente eletrónico ou digital, físico (incluindo papel), audiovisual, verbal ou outro.

Artigo 3.º

Definições

Pessoa autorizada - Qualquer pessoa a quem o Município tenha autorizado o acesso e tratamento de informação e/ou recursos do Sistema de Informação, incluindo trabalhadores, eleitos, prestadores de serviços e outros colaboradores.

Dirigente competente - Dirigente da unidade orgânica onde a pessoa autorizada está integrada ou que supervisiona as funções da pessoa autorizada, caso esta não esteja integrada em unidade com dirigente atribuído;

Sistema de Informação - Conjunto integrado de componentes para recolha, armazenamento e processamento de dados, automatizado ou não, que suportem o fornecimento de informações e conhecimento ao Município;

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;

Segurança das redes e dos sistemas de informação - A capacidade dos sistemas de rede e informação para resistir, com um dado nível de confiança, a eventos suscetíveis de pôr em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços oferecidos por esses sistemas de rede e informação, ou acessíveis por intermédio destes;

Cibersegurança - Todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas;

Confidencialidade - propriedade de que a informação apenas é acedida por quem formalmente autorizado, não sendo disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados;

Integridade - Propriedade da exatidão da informação e dos seus métodos de processamento;

Disponibilidade - Propriedade de ser acessível e utilizável quando necessária por uma entidade, processo ou pessoa formalmente autorizada;

Ativo – Todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços;

Ativo Essencial – todo o Ativo que suporte um serviço essencial prestado pelo Município;

Dispositivo móvel – no âmbito do presente Regulamento por dispositivo móvel entende-se qualquer computador portátil, tablet, smartphone ou similar, propriedade do Município ou não, que seja utilizado para acesso, processamento ou armazenamento de informação detida pelo Município.

Fornecedor - Entidade ou pessoa que fornece um produto/serviço, (sendo o produto, entendido como resultado de um processo);

Incidente - Um evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou dos serviços oferecidos por redes e sistemas de informação ou acessíveis por intermédio destas;

Tratamento de incidentes - Todas as ações e procedimentos que visam a prevenção, a deteção, a análise, a contenção ou a recuperação de um incidente;

Política - Intenções e orientação de uma entidade, conforme formalmente expressas

Metadados – descrição ou conjunto de características de um dado ou de um item, especialmente em relação à informação processada por computador, como, por exemplo, o tamanho ou o tipo de um ficheiro, ou ainda a data da última alteração;

Violação de dados pessoais - uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

CAPÍTULO II - GESTÃO DA SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Artigo 4º

Finalidade e princípios de gestão

1 — A Gestão da Segurança da Informação e Cibersegurança no Município de Valpaços assegura a definição de responsabilidades, a afetação de recursos e a supervisão do cumprimento do presente Regulamento, promovendo a proteção da informação e a resiliência das redes e sistemas de informação municipais.

2 — A implementação das medidas de segurança é realizada de forma proporcional ao contexto do Município e ao risco, em alinhamento com o quadro legal aplicável em matéria de cibersegurança e respetiva regulamentação complementar aplicável, na versão vigente.

Artigo 5º

Competências do Executivo

1 — Compete ao Executivo, no âmbito da Segurança da Informação e Cibersegurança:

a) Assegurar a disponibilização de recursos adequados ao cumprimento das obrigações legais aplicáveis em matéria de cibersegurança;

b) Determinar as orientações estratégicas e prioridades para a Segurança da Informação e Cibersegurança do Município;

c) Aprovar e promover a aplicação das políticas internas relevantes, incluindo a Política de Segurança da Informação;

d) Assegurar a realização regular de ações de sensibilização e formação em cibersegurança, promovendo uma cultura de segurança e boas práticas de gestão do risco;

e) Designar o Responsável de Cibersegurança e o(s) Ponto(s) de Contacto Permanente;

Artigo 6º

Competências dos Dirigentes

1 — Compete aos Dirigentes que superintendem as pessoas autorizadas:

a) Definir as necessidades de acesso às componentes do sistema de informação e o respetivo perfil de permissões, garantindo que os acessos são atribuídos de acordo com a necessidade de conhecer e necessidade de uso;

b) Comunicar ao Gabinete de Informática as necessidades de criação, alteração ou revogação de acessos, assegurando que tal comunicação é efetuada por meio que crie registo auditável;

c) Assegurar, nas respetivas unidades orgânicas, o cumprimento do presente Regulamento, incluindo por prestadores de serviços/avençados sob sua responsabilidade;

d) Promover a participação da respetiva unidade nas ações de sensibilização e formação em matérias de cibersegurança e proteção de dados pessoais.

Artigo 7º

Competências gerais do Gabinete de Informática

1 — O Gabinete de Informática é a unidade organizacional responsável pela gestão técnica do sistema de informação municipal, competindo-lhe, em termos gerais:

a) Assegurar a operação e manutenção das componentes digitais do sistema de informação, incluindo a gestão de utilizadores, perfis e credenciais, com base na informação transmitida pelos dirigentes;

b) Manter listagens atualizadas de utilizadores das componentes digitais do sistema de informação e promover mecanismos de revisão periódica;

c) Designar recursos com responsabilidades de administração técnica, incluindo a gestão de acessos privilegiados;

d) Acompanhar orientações técnicas e alertas de segurança emitidos pela autoridade competente e promover a sua aplicação no contexto municipal;

e) Participar na elaboração e atualização do Plano de Segurança adequando-o ao contexto do Município e ao horizonte de ameaças avaliado;

f) Detetar, mitigar e notificar incidentes de segurança nos termos do quadro legal vigente, incluindo o Regime Jurídico da Cibersegurança e colaborar na notificação de incidentes que envolvam violação de dados pessoais, tal como definido no Regulamento Geral Sobre a Proteção de Dados;

g) Controlar o acesso físico aos equipamentos informáticos que estão sob sua gestão direta, concretamente no âmbito da sala de centro de dados principal.

Artigo 8º

Responsável de Cibersegurança

1 — O Município designa um Responsável de Cibersegurança, com competências de coordenação e apoio à gestão da segurança da informação e cibersegurança, em articulação com o Executivo, Dirigentes e Gabinete de Informática.

2 — O Responsável de Cibersegurança tem, pelo menos, as seguintes competências, adequadas ao contexto do Município:

a) Participar na gestão do risco de cibersegurança do Município, propondo e acompanhando medidas de redução do risco, incluindo as relativas à cadeia de fornecimento;

b) Apoiar o Executivo e Dirigentes no exercício das suas responsabilidades em matéria de cibersegurança, assegurando a prestação de informação sobre o estado das medidas, recomendações e orientações aplicáveis;

c) Promover a cultura de cibersegurança, em estreita colaboração com o Executivo e Dirigentes, incluindo a proposta e acompanhamento de ações de sensibilização e formação;

d) Coordenar a articulação com o(s) Ponto(s) de Contacto Permanente, garantindo consistência no encaminhamento interno de informação relevante e no alinhamento com os procedimentos internos aplicáveis.

Artigo 9º

Ponto de Contacto Permanente

1 — O Município assegura a função de Ponto de Contacto Permanente, que pode ser assegurada por um elemento ou equipa.

2 — Compete aos Pontos de Contacto Permanente:

a) Assegurar a articulação operacional e técnica com a autoridade de cibersegurança competente, incluindo a obtenção, atualização e partilha de informação de situação no contexto de incidentes e respostas coordenadas;

b) Assegurar a partilha e operacionalização de informação quando estejam em vigor mecanismos ou planos de emergência com impacto no funcionamento das redes e sistemas de informação municipais;

c) Assegurar a receção e encaminhamento interno de orientações, recomendações e instruções técnicas relevantes.

CAPÍTULO III - GESTÃO DO RISCO

Artigo 10.º

Gestão do risco de cibersegurança

1 — O Município estabelece e mantém um processo de gestão do risco de cibersegurança aplicável às redes e sistemas de informação e aos ativos de informação sob sua responsabilidade, visando proteger a confidencialidade, integridade e disponibilidade da informação e assegurar a continuidade dos serviços municipais.

2 — O processo referido no número anterior inclui, pelo menos, a identificação, avaliação e tratamento do risco, bem como a monitorização e revisão periódica da eficácia das medidas implementadas.

3 — Após o tratamento do risco, o Município avalia o risco residual e determina a necessidade de medidas adicionais ou a respetiva aceitação, nos termos definidos internamente.

Artigo 11.º

Medidas mínimas, cadeia de fornecimento e documentação de suporte

1 — O Município define e implementa medidas mínimas de cibersegurança adequadas ao seu contexto e ao risco, em alinhamento com o Quadro Nacional de Referência para a Cibersegurança (QNRCS) e com a regulamentação e atos aplicáveis da autoridade competente, na versão vigente.

2 — O Município integra requisitos de segurança da informação e cibersegurança na cadeia de fornecimento, assegurando, de forma proporcional ao risco, a definição de requisitos contratuais, o controlo de acessos de fornecedores e a clarificação de responsabilidades.

3 — O Município assegura a existência e manutenção de políticas e plano(s) de segurança e promove ações de sensibilização e formação em cibersegurança, nos termos do presente Regulamento.

CAPÍTULO IV - GESTÃO DA INFRAESTRUTURA E SERVIÇOS TIC

Artigo 12.º

Gestão da infraestrutura física e parque informático

1 — Infraestrutura física

a) A gestão da segurança da infraestrutura física que suporta serviços essenciais, incluindo os necessários para o fornecimento de água potável, é da responsabilidade de cada Dirigente, no âmbito da respetiva área funcional.

b) Cada Dirigente deve assegurar a implementação e manutenção de controlos de segurança física adequados ao risco, incluindo, quando aplicável:

- controlo de acessos a instalações e áreas técnicas (salas técnicas, bastidores, asas de máquinas, captações/estações elevatórias/ETA, sistemas de telegestão e outras áreas com equipamentos críticos), com regras de autorização e registo;
- gestão de visitantes e terceiros, assegurando acompanhamento quando necessário e registo de acessos;
- proteção contra ameaças físicas e ambientais (p. ex., intrusão, incêndio, inundação e falhas elétricas), na medida aplicável às instalações;
- reporte de anomalias e articulação com as unidades competentes para correção atempada.

2 — Infraestrutura digital

a) O Município mantém um inventário dos ativos respeitante a tecnologias de informação e comunicação essenciais para a prestação de serviços enquanto autarquia local.

b) A ligação de novos equipamentos à rede interna do Município depende de solicitação prévia por escrito do dirigente competente ao Gabinete de Informática.

c) O acesso de dispositivos externos, quando autorizado, é efetuado através de zona de rede interna com separação lógica específica, definida pelo Gabinete de Informática.

d) A realocação de equipamentos informáticos só pode ser efetuada mediante pedido do dirigente competente e autorização do Gabinete de Informática. e do Departamento de Finanças e Património, para atualização do registo de inventário.

e) Os equipamentos em fim de uso devem ser entregues ao Gabinete de Informática. para execução dos procedimentos aplicáveis de remoção de dados.

Artigo 13.º

Gestão de utilizadores e acessos

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

2 — A atribuição de direitos de acesso é efetuada por perfis e privilégios mínimos, de acordo com a necessidade de conhecer e necessidade de uso.

3 — A criação, alteração ou revogação de acessos é executada pelo Gabinete de Informática com base na informação transmitida pelos dirigentes por meio que crie registo auditável.

Artigo 14.º

Repositórios digitais e cópias de segurança

1 — O Município promove a implementação de repositórios digitais centralizados.

2 — O Gabinete de Informática é responsável pela criação, gestão, atribuição de acessos e manutenção de repositórios digitais, mediante comunicação dos dirigentes.

3 — O Gabinete de Informática define, mantém e monitoriza procedimentos de cópia de segurança (backup) adequados, garantindo, de forma proporcional ao risco, a integridade e disponibilidade da informação e dos ativos selecionados.

4 — As pessoas autorizadas devem utilizar os repositórios/diretorias atribuídos, garantindo que a informação relevante se encontra em servidores centralizados abrangidos pelos procedimentos de backup em vigor.

5 — A informação relevante para a atividade do Município deve ser mantida em diretoria acessível pela pessoa autorizada e por, pelo menos, um dirigente, assegurando o acesso a informação institucional em caso de ausência.

Artigo 15.º

Gestão de Vulnerabilidades e Atualizações de Segurança

1 — O Gabinete de Informática assegura a gestão de vulnerabilidades e a aplicação de atualizações de segurança aos sistemas e serviços sob administração municipal, de acordo com a criticidade e o risco.

2 — A gestão referida no número anterior inclui, designadamente:

f) a monitorização de alertas e recomendações técnicas relevantes;

g) a avaliação do impacto e prioridade de correção;

h) a aplicação de atualizações e correções de segurança (patches) em prazo adequado ao risco;

i) o registo das intervenções efetuadas, quando aplicável.

3 — Sempre que necessário, o Gabinete de Informática pode definir janelas de manutenção e medidas de mitigação temporárias, visando reduzir a exposição a vulnerabilidades até à correção definitiva.

Artigo 16.º

Serviço de correio eletrónico institucional

1 — O Município disponibiliza às pessoas autorizadas uma caixa de correio eletrónico institucional, a qual é solicitada pelo dirigente competente, no âmbito do pedido de atribuição de acessos às componentes do sistema de informação.

2 — O acesso à componente de administração do serviço de correio eletrónico do Município está reservado, em exclusivo, ao Gabinete de Informática, abrangendo, designadamente, a criação, manutenção, suspensão e eliminação de caixas de correio eletrónico e a gestão de atributos gerais do serviço.

3 — O Gabinete de Informática promove ações de sensibilização para o uso seguro do correio eletrónico institucional.

4 — Em caso de suspensão ou término da relação contratual da pessoa utilizadora do serviço de email:

a) O utilizador diligencia no sentido de remeter ao dirigente competente da unidade orgânica, toda a informação institucional existente na respetiva caixa de correio eletrónico que considere relevante para as atividades do Município;

b) O utilizador ativa uma resposta automática normalizada, indicando um contacto alternativo definido pelo dirigente competente.

6 — O dirigente competente:

c) Indica ao utilizador qual a caixa de correio eletrónico institucional a indicar como contacto alternativo na resposta automática;

d) Assegura as diligências adequadas para garantir que a caixa de correio eletrónico a eliminar não contém informação relevante para as atividades do Município.

7 — Sem prejuízo do disposto nos números anteriores, a eliminação de caixas de correio eletrónico institucionais é efetuada pelo Gabinete de Informática, em regra, no prazo de trinta dias após o término efetivo da relação contratual, salvo determinação interna em contrário, de responsabilidade exclusiva do Presidente da Câmara.

8 — A comunicação institucional com terceiros deve, sempre que possível, ser operacionalizada através de caixa de correio de unidade orgânica ou lista de distribuição, em detrimento de conta nominal (ex: informatica@valpacos.pt).

Artigo 17.º

Acessos remotos (utilizadores e prestadores de serviços)

1 — O acesso remoto às redes e sistemas de informação do Município é disponibilizado e administrado pelo Gabinete de Informática, através de soluções autorizadas e geridas pelo Município.

2 — O Gabinete de Informática define e aplica regras técnicas e organizacionais para acessos remotos, assegurando, designadamente:

a) a atribuição e revogação de acessos remotos com base em pedido e validação do dirigente competente;

b) a limitação de privilégios e acessos ao estritamente necessário;

c) o registo e rastreabilidade dos acessos remotos;

d) condições de acesso remoto por prestadores de serviços, incluindo requisitos de autorização, delimitação de âmbito e cessação do acesso após o termo da necessidade. O acesso remoto por prestadores de serviço deve ser regulado e comunicado em momento prévio à efetivação da relação contratual.

3 — A pessoa autorizada deve utilizar o acesso remoto apenas através das soluções disponibilizadas e geridas pelo Gabinete de Informática, e não deve recorrer a soluções alternativas ou redes inseguras quando tal comprometa a segurança do acesso.

Artigo 18.º

Monitorização e registos

1 — O Gabinete de Informática é responsável pela promoção da segurança da infraestrutura institucional com recurso a ferramentas automatizadas de inspeção de tráfego e deteção de intrusões, com vista à deteção e bloqueio de tráfego potencialmente malicioso e tentativas de acesso não autorizadas.

2 — O acesso aos dados resultantes de processos de monitorização só pode ser efetuado com recurso a contas nominais ou de identificação unívoca, garantindo-se rastreabilidade por criação de logs, incluindo, pelo menos, informação sobre quem acedeu, data e hora e operações efetuadas; os logs devem, sempre que possível, ser assinados digitalmente.

3 — Os registos de atividade (logs) devem ser armazenados em modo de leitura, sendo englobados e assinados digitalmente com periodicidade máxima de um mês, por forma a constituir garantia de integridade.

4 — Os logs devem ser arquivados durante o período prescrito por diploma legal vigente, quando aplicável.

Artigo 19.º

Apoio técnico

1 — O Gabinete de Informática atua de forma autónoma ou articulada com fornecedores externos para ultrapassar condições anómalas na utilização dos sistemas informáticos.
2 — A comunicação preferencial para efeitos de apoio (helpdesk) é feita por via eletrónica, através do formulário eletrónico próprio disponível na intranet, originando registo eletrónico para suporte e controlo interno.

3 — As assistências são, sempre que possível, realizadas por acesso remoto, estando os recursos do Gabinete de Informática autorizados a ligar-se aos postos apenas para resolução de problema ou incidente reportado.

4 — Para pedidos urgentes, quando o serviço esteja paralisado ou esteja em causa a segurança do sistema informático, deve ser utilizado contacto telefónico.

CAPÍTULO V - REGRAS DE USO ACEITÁVEL

Artigo 20.º

Princípios gerais e deveres

1 — A pessoa autorizada deve utilizar os recursos do Sistema de Informação exclusivamente no âmbito das suas funções e de acordo com o presente Regulamento.

2 — A pessoa autorizada deve proteger a informação do Município, respeitando os princípios de confidencialidade, integridade e disponibilidade.

3 — A pessoa autorizada não deve contornar, desativar ou interferir com mecanismos de segurança implementados pelo Município, nem praticar atos de interferência ou interceção não autorizada sobre dados, comunicações, sistemas ou serviços.

Artigo 21.º

Gestão de Acessos

1 - A pessoa autorizada **deve**:

a) Utilizar credenciais de acesso fortes e difíceis de adivinhar, evitando palavras comuns, datas ou elementos facilmente associáveis;

b) Manter as credenciais de acesso confidenciais, guardando-as apenas em meios seguros (ex: gestor de palavras-passe ou ficheiro protegido com palavra-passe com acesso restrito);

c) Alterar a palavra-passe de acordo com os procedimentos comunicados pelo Gabinete de Informática;

d) Alterar imediatamente a palavra-passe e contactar o Gabinete de Informática sempre que exista suspeita de comprometimento da conta;

e) Bloquear o ecrã ou terminar sessão sempre que se ausente do posto de trabalho, mesmo que por períodos curtos.

2 - A pessoa autorizada **não deve**:

a) Reutilizar, para fins pessoais, palavras-passe usadas nos sistemas do Município;

b) Partilhar credenciais de acesso com terceiros, sendo responsável pela utilização efetuada através das mesmas;

c) Registar palavras-passe em papel ou mantê-las em locais visíveis;

d) Associar contas pessoais (Gmail, ou similar) a sistemas do Município quando tal permita gravação automática de palavras-passe no navegador;

e) Utilizar recursos informáticos que não lhe estejam atribuídos, ou aos quais não deva aceder, no exercício das suas funções.

3 - A pessoa autorizada é responsável por toda a atividade realizada com as suas credenciais de acesso.

Artigo 22.º

Uso do Correio Eletrónico

1 - A pessoa autorizada **deve**:

a) Usar o correio eletrónico institucional no âmbito das suas funções e de acordo com os princípios de ética e conduta aplicáveis;

b) Analisar os e-mails recebidos, antes de os utilizar, procurando sinais de phishing/fraude, nomeadamente:

- Remetente ou domínio desconhecido/suspeito;
- Pedido inesperado ou fora do procedimento habitual;
- Sentido de urgência injustificado;
- Ligações (URL) longas, complexas ou incoerentes com o contexto;

c) Confirmar, antes do envio, se o(s) destinatário(s) estão corretamente preenchidos;

d) Comunicar ao Encarregado de Proteção de Dados qualquer envio para destinatário errado quando a mensagem contenha dados pessoais;

e) Avaliar o reencaminhamento de mensagens com histórico/cadeias, assegurando que apenas é partilhada a informação necessária e com destinatários autorizados.

2 - A pessoa autorizada **não deve**:

a) Abrir anexos ou clicar em ligações de e-mails suspeitos ou provenientes de remetente desconhecido/suspeito;

b) Abrir anexos ou clicar em ligações de e-mails provenientes de remetente conhecido quando o pedido seja não habitual, incoerente ou inesperado;

c) Usar o e-mail institucional para registo em redes sociais, plataformas ou sítios web não relacionados com o exercício de funções;

d) Reencaminhar o e-mail institucional para contas pessoais, nem usar contas pessoais para fins profissionais;

e) Usar o e-mail institucional para fins incompatíveis com o exercício da atividade do Município, incluindo atividades comerciais privadas;

f) Criar ou distribuir mensagens disruptivas ou ofensivas, incluindo conteúdos discriminatórios, pornográficos ou contrários ao respeito devido;

g) Reencaminhar mensagens de acesso restrito ou que contenham informação confidencial para destinatários não expressamente autorizados.

Artigo 23.º

Gestão da transferência e partilha de informação

1 - A pessoa autorizada **deve**:

a) Usar exclusivamente as soluções de transferência e partilha de ficheiros disponibilizadas e geridas pelo Gabinete de Informática;

b) Garantir confidencialidade sobre qualquer informação obtida, acedida ou sobre a qual tome conhecimento no desempenho da atividade ao serviço do Município, quando não seja de conhecimento público;

c) Garantir confidencialidade da informação respeitante à vida privada de outros colaboradores do Município;

d) Abster-se de comentar informações de carácter institucional ou profissional em locais sem garantia de reserva de privacidade;

e) Fazer a manutenção periódica do diretório pessoal, evitando a acumulação de informação não necessária;

f) Garantir que documentos a publicar no site institucional, ou a enviar para terceiros, não contêm metadados com dados pessoais ou outra informação não relevante para a finalidade de partilha ou publicação;

g) Guardar a informação institucional nos repositórios/diretorias autorizados, assegurando que a informação relevante se encontra acessível pela própria e por, pelo menos, um dirigente, quando aplicável.

2 - A pessoa autorizada **não deve**:

a) Enviar informação do Município para clouds públicas ou plataformas similares com as quais o Município não tenha serviços contratualizados, incluindo o uso de soluções do tipo WhatsApp para registo e partilha de cópias de documentos obtidos em contexto profissional;

b) Usar suportes amovíveis com capacidade de armazenamento de dados (pen USB, discos externos) para recolha e armazenamento de informação do Município sem autorização do Gabinete de Informática;

c) Transferir informação confidencial para computador ou dispositivo móvel que não seja do Município, salvo autorização e condições definidas;

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 desnecessariamente pesados (fotografias com resolução elevada), devendo restringir-se ao estritamente necessário para suporte das tarefas institucionais;

f) Proceder, por iniciativa própria, à remoção/eliminação de dados em equipamentos em fim de uso, devendo entregar os mesmos ao Gabinete de Informática para execução dos procedimentos aplicáveis.

Artigo 24.º

Rede e Equipamentos Informáticos

1 - A pessoa autorizada **deve**:

a) Fazer um uso adequado dos recursos disponibilizados pelo Município (rede, aplicações e equipamentos), evitando consumos desproporcionais que impactem outros utilizadores.

b) Terminar sessão e encerrar aplicações/serviços no final do uso;

c) Desligar os equipamentos utilizados, incluindo computadores, sempre que ocorra uma pausa prolongada e, obrigatoriamente, no final do dia de trabalho, salvo necessidade operacional autorizada pelo Gabinete de Informática;

d) Solicitar autorização ao Gabinete de Informática para qualquer necessidade de realocação de equipamentos ou dispositivos;

e) Informar o Gabinete de Informática sempre que identifique comportamentos inesperados ou anormais no dispositivo, na rede ou no acesso à Internet.

2 - A pessoa autorizada **não deve**:

a) Proceder à ligação de novos equipamentos à rede interna do Município sem prévia autorização do Gabinete de Informática;

b) Utilizar recursos informáticos do Município para fins comerciais ou pessoais não relacionados com o exercício de funções;

c) Instalar aplicações, software executável ou similar, nem alterar configurações de sistemas ou aplicações instaladas, sem autorização do Gabinete de Informática.

Artigo 25.º

Acesso à Internet e Serviços Web

1 - A pessoa autorizada **deve**:

a) Usar apenas software e ferramentas de acesso à Internet autorizados pelo Município;

b) Inserir informação em sites e plataformas de entidades públicas e privadas com quem o Município mantenha relações contratuais ou institucionais, quando tal seja necessário ao desempenho de funções;

c) Contactar o Gabinete de Informática sempre que um site ou plataforma apresente comportamento não esperado, pedidos anormais ou sinais de risco de segurança.

2 - A pessoa autorizada **não deve**:

a) Introduzir informação do Município, não manifestamente de carácter público, incluindo dados pessoais, em soluções de inteligência artificial generativa, salvo autorização e condições definidas pelo Município;

b) Aceder a sites ou aplicações com conteúdo inapropriado ou ofensivo, não condizentes com o desempenho das funções;

c) Recorrer a aplicações ou mecanismos destinados a contornar as restrições de acesso definidas pelo Município;

d) Aceder a sites ou aplicações que consumam recursos de rede excessivos, tais como plataformas de *streaming* de média e jogos online;

e) Transferir material protegido por direitos de autor.

Artigo 26.º

Espaço de Trabalho e Documentos Físicos

1 - A pessoa autorizada **deve**:

a) Assegurar que os documentos em formato físico são conservados de forma a prevenir acesso não autorizado, particularmente em zonas do edificado 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 terceiros não autorizados;

d) Tomar medidas adequadas para preservar a segurança de documentos em contexto de transporte fora dos espaços físicos do Município, prevenindo perdas e acessos não autorizados;

e) Usar o código de utilizador atribuído para ativação do sistema de impressão em uso no Município, sendo responsável pelo seu uso indevido em caso de cedência a terceiros;

f) 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 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 aplicável.

Artigo 27.º

Acesso remoto e teletrabalho

1 - A pessoa autorizada **deve**:

a) Cumprir as orientações do Município para acesso remoto e teletrabalho, protegendo credenciais e informação do Município;

b) Garantir que a informação tratada em teletrabalho é mantida protegida contra acesso por terceiros não autorizados;

c) Reportar ao Gabinete de Informática qualquer anomalia, suspeita de incidente ou perda/roubo de equipamento usado em contexto de acesso remoto.

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) Armazenar, de forma permanente, informação do Município em equipamento pessoal, salvo autorização e condições definidas.

Artigo 28.º

Dispositivos móveis

1 - A pessoa autorizada **deve**:

a) Ativar palavra-passe, PIN ou equivalente, para autenticação e acesso ao dispositivo móvel;

b) Ativar as ligações Wi-Fi e Bluetooth apenas quando estritamente necessário;

c) Ativar o bloqueio automático do dispositivo em caso de inatividade;

d) Manter, sempre que tecnicamente possível, a informação do Município armazenada em dispositivos móveis protegida por mecanismos de segurança adequados, incluindo encriptação;

e) Notificar o Gabinete de Informática em caso de perda ou roubo de dispositivo móvel do Município, ou de dispositivo que contenha informação do Município.

2 - A pessoa autorizada **não deve**:

a) Transmitir credenciais de acesso ou outros métodos de autenticação associados ao dispositivo móvel a terceiros, incluindo familiares;

b) Deixar o dispositivo móvel em veículos sem vigilância;

c) Ligar-se a redes Wi-Fi públicas que não apresentem garantias de segurança adequadas.

CAPÍTULO VI – INCIDENTES, AUDITORIA E DISCIPLINA

Artigo 29. °

Notificação e registo de incidentes

1 — A pessoa autorizada tem o dever de comunicar superiormente qualquer tentativa de acesso não autorizado ou qualquer uso indevido de recursos digitais ou físicos do sistema de informação.

2 — O testemunho direto, ou a tomada de conhecimento indireta, de incidentes relacionados com a segurança, uso abusivo de recursos ou incumprimento do presente Regulamento deve ser comunicado ao superior hierárquico ou ao Gabinete de Informática.

3 — As notificações de incidentes devem ser registadas através da ferramenta interna de pedidos de suporte ao Gabinete de Informática.

Artigo 30. °

Tratamento de incidentes e preservação de evidências

Encarregado de Proteção de Dados, para avaliação do risco e de eventuais obrigações de notificação às autoridades competentes e aos titulares dos dados, nos termos aplicáveis.

Artigo 31. °

Auditoria

1 — O cumprimento do presente Regulamento, incluindo a atividade realizada pela pessoa autorizada nos equipamentos informáticos do Município, pode, em qualquer altura, ser objeto de auditoria, pelo Gabinete de Informática sob coordenação do Responsável de Cibersegurança designado, para garantir o cumprimento das normas de uso e assegurar a qualidade e o bom funcionamento dos serviços de tecnologias de informação e comunicação.

2 — As auditorias internas devem ser complementadas por auditorias externas, abrangendo o âmbito do Plano de Segurança e incluindo o cumprimento do presente Regulamento, sendo supervisionadas pelo Responsável de Cibersegurança designado.

3 — A informação constante do relatório de auditoria é considerada confidencial, não podendo ser utilizada para outros fins sem prévia autorização do Responsável de Cibersegurança.

Artigo 32. °

Regime disciplinar

O incumprimento 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.

CAPÍTULO VII - DISPOSIÇÕES FINAIS

Artigo 33.º

Procedimento, comunicação e localização do Regulamento

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

Artigo 34.º

Aprovação do Regulamento

O presente Regulamento foi aprovado pela Câmara Municipal de Valpaços, no dia 18 de junho no seguimento de proposta do Responsável de Cibersegurança.

Artigo 35.º

Revisão do presente regulamento

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

Artigo 36.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 Valpaços.

Artigo 37.º

Entrada em vigor

O presente documento entre em vigor 5 dias após a deliberação de aprovação tomada pela Câmara Municipal.