EDITAL

-AMILCAR RODRIGUES CASTRO DE ALMEIDA- Presidente da Câmara Municipal de Valpaços.----------

-Torna público: que a Câmara Municipal em reunião ordinária realizada no dua 19 de junho de 2023 deliberou, por unanimidade, aprovar o Regulamento de Segurança do sistema de Informação do Municipio de Valpaços, que junto se anexa.----------

E para constar vai o mesmo ser publicado no sitio institucional do Municipio e disponibilizado na intranet e enviado por e-mail, para todas as pessoas utilizadoras.----------

Paços do Concelho de Valpaços, 19 de junho de 2023.

O Presidente da Câmara Municipal

Dr. Amílcar Rodrigues Castro de Almeida

CÂMARA MUNICIPAL DE VALPAÇOS
Presente à reunião de 19/06/2023
Deliberado por unanimidade, aprovar o Regulamento de Segurança do Sistema de Inf. do Município de Valpaços e proceder à sua publicação nos termos legais.

Regulamento de Segurança do Sistema de Informação do Município de Valpaços

Versão 1.0

Data: Junho 2023

INDICE

Regulamento de Segurança do Sistema de Informação do Município de Valpaços

Preâmbulo

A informação, nos seus vários formatos, desempenha um papel fundamental cuja crescente importância perpassa a sociedade atual. No cumprimento das funções de promoção e salvaguarda dos interesses próprios das respetivas populações, cabe às Autarquias locais responsabilidade acrescida no que respeita à gestão do ciclo de vida de toda a informação.

Dando cumprimento aos compromissos assumidos em sede de Politica de Segurança da Informação, elaborada em linha com os avanços legislativos nacionais: Lei 46/2021 e Decreto-lei 65/2021, e europeus: Diretiva (EU) 2022/2555, o Municipio de Valpaços visa com a apresentação do presente Regulamento de Segurança do Sistema de Informação, garantir a confidencialidade, integridade e disponibilidade da informação, incluindo dados pessoais, evitando que esta seja, de modo acidental ou ilícito, perdida, destruída, alterada indevidamente ou acedida por quem não autorizado. Para tal, com este documento estabelecem-se os direitos e deveres dos utilizadores do Sistema de Informação do Município em todas as suas componentes, digitais e físicas. Consequentemente pretende o mesmo definir responsabilidade disciplinar ou criminal determinando, desta forma, o poder de auditoria em sede de regime disciplinar, dando total cumprimento às disposições legais aplicáveis relativas à criminalidade informática, à proteção de dados pessoais, ao regime jurídico da segurança do ciberespaço.

CAPÍTULO I - DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto do Regulamento

O presente Regulamento objetiva definir as regras e práticas para assegurar a garantia de confidencialidade, privacidade, integridade, disponibilidade da informação gerida pelo sistema de informação do Município de Valpaços com vista à prevenção de ocorrência e mitigação do impacto de eventuais incidentes que possam comprometer o regular funcionamento da autarquia, a violação da privacidade de dados pessoais e a demonstração permanente de conformidade legal aplicável ao município

O disposto no presente Regulamento observa de forma estrita a conformidade com a legislação e normativos em vigor em matéria de proteção de dados pessoais, criminalidade informática e segurança de redes, sistemas de informação e Cibersegurança, respetivamente, Regulamento (UE) 679/2016 de 27 de abril, Regulamento Geral sobre a Proteção de Dados, RGPD, Lei 58/2019 de 8 de agosto, execução nacional do RGPD, Lei n.º 46/2018 de 13 de agosto – Regime Jurídico da Segurança do Ciberespaço, Decreto Lei 65/2021 de 30 de julho e Lei 109/2009 de 15 de Setembro – Lei do Cibercrime.

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 Valpaços, **independentemente do seu formato físico ou digital**, com o objetivo de orientar ou 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 Valpaços, independentemente do seu suporte de registo: **eletrónico ou digital, físico (incluindo papel), audiovisual, verbal ou outro.**

Artigo 3.º

Definições

Regulamento da Segurança do Sistema de Informação – Documento que orienta ou regula as práticas que as pessoas ou sistemas no domínio da segurança do sistema de informação devem executar nas suas ações diárias;

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 a uma organização;

Confidencialidade - propriedade de que a informação apenas é acedida pelas pessoas formalmente autorizadas, 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 ou pessoa formalmente autorizada;

Não repudio – garantia que todos os utilizadores quando na condição de emissores de informação ou quando partilham dados pessoais com destinatários autorizados, serão sempre identificados física e/ou digitalmente com valor probatório legal.

Segurança de Sistemas de Informação – enquadramento organizacional de cultura, políticas, processos, procedimentos e estruturas organizacionais e ambiente operacional utilizado para assegurar a confidencialidade, privacidade, integridade, e disponibilidade da informação essencial de uma organização:

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;

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;

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;

Ativo – qualquer coisa que tenha valor para a organização;

Ativo Essencial – componente do sistema de informação, hardware, software ou aplicação que suporte um serviço essencial prestado pelo Município;

Dono do Ativo - recurso interno responsável por um ativo;

Incidente - um evento com um efeito adverso na segurança das redes e dos sistemas de informação;

Tratamento de incidentes - todos os procedimentos de apoio à deteção, análise, contenção e resposta a um incidente.

Informação e ativo essenciais – Informação e recursos que têm um valor crítico para o Município como suporte para o normal desenvolvimento das suas atividades.

Artigo 4.º

Pessoa autorizada

Consideram-se pessoa autorizada para efeitos do presente documento, as/os funcionárias/os do município, as/os contratada/o(s), as/os eleitos locais e outros agentes que utilizem recursos da autarquia ou pessoais para aceder, armazenar, fazer *backup* ou realocar qualquer informação da autarquia.

CAPÍTULO II - GESTÃO DE ACESSOS

Artigo 5º

Acesso à informação

O Município de Valpaços restringe o acesso à informação através da aplicação de controlos de acesso lógicos e físicos que garantam que:

- O acesso à informação está restrito a quem necessita de a conhecer para a prossecução das suas competências - Necessidade de Conhecer;
- 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 - Necessidade de Uso.

Artigo 6º

Responsabilidades - Município

1. O Município define e mantém um processo formal de disponibilização de contas de acesso do sistema de informação para atribuir, alterar ou revogar os direitos de acesso.
2. O acesso a componentes do sistema de informação, dispositivos, aplicações, sistemas ou similares, é feito mediante um processo de autenticação auditável. Este, pode recorrer ao uso de credenciais de acesso, como nome de utilizador e palavra-passe ou equivalente, atribuídas ao colaborador/Departamento com base em proposta do dirigente competente.
3. 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.
4. O Município aprova e comunica, perante as partes interessadas, definidas em sede de Plano de Segurança, uma Política de Segurança da Informação incluindo Cibersegurança, uma Política de Privacidade e Tratamento de Dados Pessoais.

Responsabilidades - Dirigentes

1. O dirigente que superintende cada pessoa autorizada, ou o Presidente da Camara, definem as necessidades de acesso de cada pessoa autorizada às componentes do sistema de informação e correspondente perfil de permissões. Esta necessidade é comunicada ao GI através do sistema de gestão documental recorrendo ao uso de documento validado pelo Sistema de Gestão da Qualidade, ou existindo impossibilidade de o fazer, a comunicação deve ser feita através de procedimento que crie registo auditável.

Responsabilidades – Gabinete de Informática

1. O Gabinete de Informática (GI) é a unidade organizacional responsável pela criação dos utilizadores com base na informação transmitida pelo dirigente.
2. O Gabinete de Informática mantém uma listagem atualizada dos utilizadores das componentes de carater digital do sistema de informação Municipal que recorram a meios de autenticação por utilizador e palavra-passe.
3. O Gabinete de Informática designa um número suficiente de recursos com responsabilidade de gestão de acessos privilegiados de administração de rede. As funções de administrador de rede são ratificadas pelo Presidente de Camara.
4. O Gabinete de Informática envia, via sistema de gestão documental, com periodicidade semestral, a lista de utilizadores referida no ponto 2. desta cláusula, pera o dirigente responsável de cada colaborador.
5. O acesso a partir de localizações externas ao sistema de informação do Município é feito mediante autorização do GI e através de recursos disponibilizados pelo GI.

Responsabilidades – Departamento de Administração Geral

1. O Diretor do Departamento de Administração Geral, comunica ao GI a cessão da relação laboral ou a transferência do trabalhador para outro serviço, secção ou unidade a fim de que o GI possa proceder às diligências necessárias para suspensão, cancelamento ou adequação dos acessos existentes, bem como à recolha de equipamentos ou implementação de ações de manutenção, salvaguardando informações de carater confidencial.

CAPÍTULO III - DIREITOS, DEVERES E PROIBIÇÕES

Artigo 7.º

Direitos da pessoa autorizada

1. A pessoa autorizada tem direito à liberdade e privacidade no âmbito do processamento informático dos seus dados pessoais e no âmbito do trabalho técnico da sua responsabilidade e autoria. O Município disponibiliza, sempre que possível, redes abertas para uso pessoal e cuja segurança se encontra a cargo de cada utente.
2. A pessoa autorizada tem, ainda, os seguintes direitos:
    a. Direito de informação:

        No momento da recolha de dados pessoais, ou, caso a recolha de dados não seja feita diretamente junto de si, logo que os mesmos sejam tratados, a pessoa autorizada tem o direito de ser informado sobre:

        i. Qual a finalidade do tratamento;

        ii. Quem é responsável pelo tratamento dos dados;

        iii. A quem podem ser comunicados os seus dados;

        iv. Quais as condições em que pode aceder e retificar os seus dados;

    b. Direito de oposição:

        i. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, se feito com base na prossecução do interesse público ou exercício de autoridade pública, ou feito no interesse legítimo do Município de Valpaços. O Município cessa eventual tratamento de dados pessoais, caso não apresente razões imperiosas e legítimas para esse mesmo tratamento que sobre o mesmo prevaleçam interesses, direitos e liberdades da pessoa autorizada.

Artigo 8.º

Deveres da pessoa autorizada

1. A pessoa autorizada deve respeitar sempre a liberdade e a privacidade alheias.
2. A pessoa autorizada é responsável pelo correio eletrónico originado a partir de contas de email para as quais tem autorização de uso.
3. Às proibições constantes do artigo seguinte ou estabelecidas em outros preceitos do presente documento corresponderá o correlativo dever, ainda que não expressamente enunciado.
4. Respeitar as boas práticas para a escolha ou composição de palavras-passe resilientes a ataques ou tentativas de acesso indevido, nomeadamente:
    a. Não usar como password palavras únicas do dicionário, datas, ou outras facilmente associáveis ao colaborador;

b. Manter as passwords confidenciais, guardar as passwords em software dedicado ou ficheiros cifrados com acesso restrito;
c. Não manter as passwords escritas em papéis ou locais visíveis;
d. Mudar as passwords regularmente, seguindo as orientações do Gabinete de Informática.
e. Não gravar as passwords de forma automática em aplicações acessíveis a partir de computadores partilhados;
f. As passwords de determinado sistema informático não devem ser reutilizadas em sistemas de diferente âmbito, mesmo que em contexto de uso no Município.
g. Não reutilizar passwords em uso em sistemas do Município em contextos de uso pessoal;

Artigo 9.º

Restrições com os acessos de cada pessoa autorizada

1. A pessoa autorizada não pode ceder os seus privilégios de acesso nem pode usar os privilégios de outros.
2. A pessoa autorizada é o único responsável pelo uso indevido dos seus privilégios de acesso e deverá comunicar algum uso ou suspeita de uso indevido ao seu superior hierárquico, em cadeia, bem como ao GI, em caso de suspeita de uso indevido.
3. A pessoa autorizada não deve partilhar os seus privilégios de acesso com terceiros, caso tal ocorra a pessoa autorizada é considerada o único responsável pelo uso dos mesmos.
4. A pessoa autorizada não pode efetuar acessos não autorizados.

A pessoa autorizada não deve usar recursos informáticos que não lhe estejam direta, ou indiretamente, atribuídos.

Artigo 10.º

Proibições gerais relativas à pessoa autorizada

1. A pessoa autorizada não pode interferir com dados, programas ou sistemas, nem intercetar informação de outra pessoa autorizada ou do Município.
2. A pessoa autorizada deve abster-se de tomar atitudes que possam causar prejuízos morais ou materiais às restantes pessoas autorizadas, e ao sistema de informação do Município.
3. A pessoa autorizada não pode proceder à ligação de novos equipamentos à rede interna do Municipio sem prévia solicitação do dirigente responsável por escrito ao Gabinete de Informática. O acesso de dispositivos externos, quando autorizado, é feito através de zona de rede interna com separação lógica especifica.

4. A pessoa autorizada não pode utilizar recursos informáticos do Município para fins comerciais não relacionados com o Município.

5. A pessoa autorizada não pode instalar aplicações, software executável ou similar, nem alterar a configuração das aplicações ou sistemas instalados, sem pedido prévio por escrito do dirigente responsável. Se o pedido for de forma verbal deve o GI proceder a registo escrito acessível ao dirigente.

6. A pessoa autorizada deve fazer um uso adequado dos recursos disponibilizados pelo Municipio, nomeadamente recursos de rede por forma a não consumir recursos desproporcionais a impactar o uso da rede dos outros utilizadores.

7. A realocação de equipamentos informáticos só pode ser feita mediante pedido do dirigente responsável e consequente autorização do Gabinete de Informática e do Departamento de Finanças e Patrimonio para alteração do registo de inventário existente.

8. A pessoa autorizada não deve recorrer ao uso de dispositivos amovíveis para armazenamento de informação sem pedido prévio por escrito ao Gabinete de Informática.

SECÇÃO I - DO CORREIO ELETRÓNICO (E-MAIL)

Artigo 11.º

Responsabilidades

1. O Gabinete de Informática é responsável pela gestão da infraestrutura de correio eletrónico, incluindo a implementação dos processos de criação, manutenção e criação de acessos a caixas de correio eletrónico.

2. O Gabinete de Informática deve promover ações de sensibilização para um uso seguro do sistema de correio eletrónico institucional.

3. Aquando do término de relação contratual a conta de correio eletrónico institucional será eliminada num período nunca superior a 30 dias, sendo o utilizador notificado por escrito por comunicação do Departamento de Administração Geral, através de documento dedicado, subscrito pelo dirigente respetivo. A pessoa autorizada que termina funções deve proceder ao encaminhamento de informação institucional relevante para a prossecução das atividades do Município.

   Durante um período não superior a 30 dias será implementado uma mensagem automática informando que a conta se encontra desabilitada e será indicado uma conta de correio eletrónico para contacto alternativo.

4. Dever-se-á privilegiar o uso de contas de correio eletrónico que recorram a listas de distribuição na comunicação institucional com o exterior.

5. As caixas pertencentes a utilizadores em regime de comissão serviço devem permanecer inativas durante a duração da comissão de serviço, salvo indicação por escrito do dirigente do serviço de tutela.

Artigo 12.º

Condicionantes à utilização do correio eletrónico

1. O uso do sistema de correio eletrónico institucional deve seguir os princípios gerais de Ética e Conduta aplicáveis aos trabalhadores da Administração Pública.
2. São interditos na utilização de correio eletrónico os seguintes procedimentos:
    a. Falsificar mensagens de correio eletrónico;
    b. 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;
    c. Usar o sistema de e-mail do Município de Valpaços 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;
    d. O uso do correio eletrónico institucional para fins não compatíveis com o exercício da atividade do Município, nomeadamente para atividades comerciais privadas.
    e. Reencaminhar mensagens de acesso restrito, que contenham informações confidenciais, para destinatários não expressamente autorizados a aceder à informação.

Artigo 13.º

Gestão de administrador do serviço de correio eletrónico (e-mail)

1. O acesso à componente de administração das caixas de correio eletrónico do serviço do Município, está reservado, em exclusivo, ao Gabinete de Informática. A administração está restrita à criação, suspensão, eliminação e gestão de atributos gerais do serviço de correio eletrónico.

SECÇÃO II - DA COMUNICAÇÃO E TRANSFERÊNCIA DE INFORMAÇÃO

Artigo 14.º

Transferência e partilha de informação

1. A preservação da confidencialidade das informações institucionais e da privacidade de todos que com o Município de Valpaços colaboram são princípios fundamentais devendo para isso os trabalhadores:

    a. Manter total confidencialidade sobre todas as informações acedidas ou sobre as quais tomem conhecimento no decurso do desempenho da atividade profissional ao serviço do Município.

    b. Não divulgar informação confidencial ou respeitante à vida privada de outros trabalhadores, excetuando-se todas as situações decorrentes das atividades do Município.

    c. Não abordar informações de carater institucional ou profissional em locais públicos ou privados sem garantia de reserva de privacidade.

    d. Não enviar dados do Município em suporte digital para Clouds públicas, ou plataformas de uso similar, geridas através de contas de utilizador não geridas pelo Município sem comunicação prévia e subsequente autorização por parte do GI.

SECÇÃO III - DO USO DE REPOSITÓRIOS

Artigo 15.º

Responsabilidades

1. O Município deve promover a implementação de repositórios digitais centralizados.
2. O Gabinete de Informática é responsável criação, gestão, atribuição de acessos e manutenção de repositórios digitais mediante comunicação dos dirigentes.
3. O Gabinete de Informática 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 integridade e disponibilidade.

Artigo 16.º

Uso de repositórios digitais

1. A pessoa autorizada deve usar os repositórios digitais (diretorias) atribuídas a cada Unidade Organizacional e/ou Utilizador sendo as mesmas arquivadas em servidores centralizados. Apenas sobre os mesmos é garantida a aplicação do procedimento de backup em vigor.
2. O conjunto de informação relevante para a atividade do Município deve ser mantido em diretoria acedível pela pessoa autorizada e pelo menos um dirigente, que garanta o acesso à informação em caso de ausência.

3. A pessoa autorizada que recorra a dispositivos com capacidade de armazenamento de dados em formato digital, deve entregar o equipamento em fim de uso ao GI, para que seja efetuado um procedimento de remoção de dados.
4. Os repositórios de acesso individual não devem ser usados para arquivo de dados não respeitantes à atividade do Município, nomeadamente dados do foro pessoal.

SECÇÃO IV – DO ESPAÇO DE TRABALHO E DOCUMENTOS EM FORMATO FÍSICO

Artigo 17.º

Condicionantes quanto ao espaço de trabalho

1. A pessoa autorizada deve seguir os princípios da mesa limpa e do ecrã limpo.
2. Os espaços de trabalho devem ser organizados por forma prevenir a ocorrência de violações de segurança que impliquem perdas, acessos ou alterações não autorizados, quer para informação em formato físico quer para informação em formato digital.
3. O transporte de documentos para fora do Município apenas pode ocorrer quando o mesmo decorra do exercício de funções que assim o exijam.
4. A pessoa autorizada que transporte documentos para fora dos espaços físicos do Município de Valpaços deve tomar medidas adequadas para preservar a segurança dos mesmos, nomeadamente adotar procedimentos que mitiguem riscos de acesso indevido.
5. O sistema de impressão em uso no Município dispõe de sistema de ativação por código de utilizador, devendo o mesmo estar ativado sempre que tecnicamente possível. O utilizador que ceda o código a terceiros é responsável pelo seu uso indevido incluindo acesso não autorizado a documentos.
6. A destruição de documentos em suporte físico deve ser feita com recurso a meios adequados que impossibilitem a reconstituição de documentos, nomeadamente destruidoras de papel.

Artigo 18.º

Proibições relativas à pessoa autorizada

1. A pessoa autorizada não pode fazer registo fotográfico, vídeo ou similar de documentos em formato físico ou outro suporte de dados, quando não autorizado pelo respetivo dirigente.
2. O uso de sistemas de impressão e digitalização está restrito a utilizadores autorizados.

SECÇÃO V – TRABALHO REMOTO E TELETRABALHO

Artigo 19.º

Acesso remoto

1. O acesso em modo remoto ao sistema de informação do Município é feito em exclusivo através das soluções providas e geridas pelo Gabinete de Informática.
2. O acesso ao sistema de informação deve ser operacionalizado de forma que aplicações e sistemas produtivos a usar para processar dados estejam no perímetro físico do Município ficando o utilizador restrito ao acesso a um *front office* do sistema.
3. A utilização de acessos remotos só é concretizada mediante informação escrita do dirigente ao Gabinete de Informatica que identifique o utilizador e os recursos internos do sistema de informação aos quais deve ser concedido acesso e a duração prevista.
4. O Gabinete de Informática mantém uma lista de acessos remotos autorizados que inclua a data de atribuição e data de revogação.

Artigo 20.º

Teletrabalho

1. A execução de funções em formato teletrabalho requer autorização prévia do Presidente de Câmara.
2. O Presidente da Câmara, comunica ao Gabinete de Informática que disponibilize ao trabalhador/a em teletrabalho, meios de suporte ao exercício de funções que apliquem os mesmos níveis de acesso que o trabalhador/a mantinha em trabalho presencial.
3. O Gabinete de Informática realiza uma sessão prévia com o/a trabalhador/a para apresentação do funcionamento do sistema a usar bem como das regras de segurança a seguir.
4. O/A trabalhador/a em teletrabalho não deve manter quaisquer dados no equipamento em uso para acesso remoto.

SECÇÃO VI – DISPOSITIVOS MÓVEIS

Artigo 21.º

Uso de dispositivos móveis

Considera-se para efeitos do presente Regulamento, como dispositivo móvel, computador portátil em uso em formato de mobilidade, tablet, smartphones e similares, propriedade do Município ou não, que seja usado para acesso, processamento e armazenamento de informação detida pelo Município.

A pessoa utilizadora de dispositivos móveis deve garantir a implementação das medidas a seguir indicadas:

e. Uso obrigatório de Password, PIN ou equivalente, para autenticação e acesso a dispositivo;

f. Não transmitir as suas passwords e outros métodos de autenticação, a terceiros, incluindo aos membros da família e a outros trabalhadores;

g. Não deixar os equipamentos móveis em veículos automóveis sem vigilância;

h. Os dispositivos apenas devem ter as ligações Wifi e Bluetooth ativas, quando necessário;

No caso de perda ou roubo de um dispositivo móvel é obrigatória a comunicação imediata ao Gabinete de Informática.

Os dispositivos portáteis devem ter os dados encriptados sempre que seja tecnicamente possível.

CAPÍTULO IV – SEGURANÇA E MONITORIZAÇÃO

Artigo 22. °

Regime Jurídico da Segurança no Ciberespaço

1. O Município assegura a disponibilização de recursos adequados ao cumprimento das obrigações legais decorrentes do Regime Jurídico da Segurança no Ciberespaço.
2. O Município designa pontos de contactos permanente com o Centro Nacional de Cibersegurança em número suficiente para assegurar as obrigações decorrentes do quadro legal, e um Responsável pela Segurança que assuma a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes.
3. O Município define e mantem atualizado um Plano de Segurança que compreenda as principais tarefas de gestão da segurança da informação. Este integra uma Política de Segurança da Informação.
4. O GI e o Departamento de Administração Geral, definem e promovem a implementação de ações de formação sobre temáticas atinentes à Cibersegurança e proteção de dados pessoais com vista à capacitação para a segurança da informação e promoção da privacidade.

Artigo 23.°

Deveres do Gabinete de Informática

1. Cabe ao GI a obrigação de:

a. Manter um inventário de todos os ativos digitais essenciais para a prestação dos serviços do Município;

b. Participar na elaboração e atualização do Plano de Segurança adequando-o ao contexto do Municipio e ao horizonte de ameaças avaliado;

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

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

e. Aplicar e manter um processo de realização de cópias de segurança e verificar periodicamente a sua integridade;

f. Verificar os *logins,* acessos e registos de auditoria dos sistemas para controlar tentativas de violação e quebras de segurança;

g. Criar e preservar registos de incidentes de segurança por forma a facilitar analise forenses quando avaliado como necessário;

h. Acompanhar as orientações técnicas e alertas de segurança emitidos pelo Centro Nacional de Cibersegurança.

Artigo 24.º

Monitorização e criação de registos

1. **Monitorização do tráfego de rede**
   a. 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, assim com de tentativas de acesso não autorizadas;
   b. O Gabinete de Informática deve promover o uso de sistemas de controlo de tráfego que privilegiem o bloqueio em detrimento da deteção por meio de inspeção de tráfego;
   c. O acesso aos dados resultantes de processos de monitorização só poderá ser efetuado com recurso a contas de acesso nominais ou de identificação unívoca;
   d. A rastreabilidade dos acessos deve ser garantida por meio da parametrização dos sistemas para criação de *logs* de registo, incluindo, pelo menos, a informação sobre quem acedeu, data e hora, operações

efetuadas. Os *logs* devem, sempre que possível, ser assinados digitalmente.

2. **Arquivo de registos**
    a. Armazenamento em modo de leitura dos registos de atividade (*log*), devendo, com uma periodicidade máxima de um mês, ser englobados num único bloco de registos e assinado digitalmente por forma a constituir garantia de integridade.
    b. Os registos (*logs*) deverão ser arquivados durante período prescrito por diploma legal vigente, quando aplicável.

Artigo 25.º

Apoio técnico

Solicitações dos ao Gabinete de Informática - HelpDesk

1. O Gabinete de Informatica atuará de forma autónoma ou, de forma articulada com fornecedores externos, para ultrapassar quaisquer condições que se considerem anómalas na utilização dos sistemas informáticos respeitando os seguintes preceitos.
    a. A comunicação preferencial com o Gabinete de Informática para efeitos de apoio - helpdesk informático - deverá ser feita por via eletrónica através de preenchimento do formulário eletrónico próprio, disponível na intranet.
    b. Este procedimento dará origem a um registo eletrónico que servirá de suporte na resposta ao pedido e para controlo interno.
    c. Os pedidos de assistência serão, sempre que possível, realizados por acesso remoto, estando os recursos do Gabinete de Informática autorizados a ligarem-se aos postos apenas aquando da resolução de problema ou incidente reportado.
    d. Remete-se para contacto telefónico pedidos urgentes sempre que se verifique que o serviço da pessoa utilizadora se encontra paralisado por força de problema no sistema informático, ou outro, que perturbe o normal funcionamento da globalidade de um serviço ou ainda quando esteja em causa a segurança do sistema informático.

Artigo 26.°

Notificação de incidentes

1. A pessoa utilizadora do sistema tem o dever de comunicar superiormente qualquer tentativa de 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 Gabinete de Informática.
3. As notificações de incidentes devem ser executadas através da ferramenta interna de pedidos de suporte do Gabinete de Informática.

Artigo 27.°

Incidentes e suas consequências

1. Os incidentes de segurança relacionados com a componente digital do sistema de informação deverão ser comunicados através da ferramenta interna de pedidos de suporte (helpdesk) ao Gabinete de Informática competindo-lhe diligenciar pela mitigação do incidente, pelo registo de evidencias e subsequente comunicação ao responsável pela segurança conforme previsto no art.º. 19.º do D.L 65/2021.
2. Os incidentes de segurança relacionados com a componente física do sistema de informação deverão ser comunicados, aos responsáveis abaixo listados e em complemento inseridos na ferramenta interna de pedidos de suporte ao Gabinete de Informática:
    - Espaço físico da Biblioteca, Eng. Normando Viera;
    - Departamento de Obras Municipais, Eng. Durão Branco;
    - Pavilhão e Estádio Municipal, Eng. Normando Vieira;
    - Edifício das Piscinas, Eng. Normando Vieira;
    - Loja do cidadão, Vereador Eng. Jorge Pires;
    - Auditório Municipal, Eng. Normando Vieira;
    - Loja Ponto Já, Eng. Normando Viera;
    - CPCJ, Vereadora Dra. Teresa Pavão;
    - Edifício da Ação social, Eng. Normando Vieira;
    - Balcão Único do Prédio, Vereador Eng. Jorge Pires;
    - Espaço da antiga escola P3, Eng. Normando Vieira;
    - Pavilhão Multiusos, Eng. Normando Vieira;
    - Casa do Vinho, Vereador Dr. Jorge Pires;
    - Centros Escolares, Eng. Normando Vieira;
    - Edifício dos Paços do Concelho, Dr. Luis Chaves, Dr. Francisco Lavrador, Eng. Normando Vieira, Eng. Cruz, Engª Paula Magalhães;

3. As unidades orgânicas identificadas no número que antecede são responsáveis pela mitigação de incidentes sobre ativos físicos, pelo registo de evidências e subsequente comunicação ao vereador do pelouro e ao Responsável de Segurança designado.

4. Os incidentes de segurança respeitantes a intrusão, acesso indevido, sabotagem com impacto substancial em ativos de informação devem ser comunicados ao Centro Nacional de Cibersegurança. Cabe ao Responsável de Segurança a respetiva tomada de decisão com base no procedimento de gestão de incidentes existente.

CAPÍTULO V - AUDITORIA E REGIME DISCIPLINAR

Artigo 28.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, por ou sob gestão do Gabinete 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 internas devem ser complementadas por auditorias externas, que abranjam todo o âmbito do Plano de Segurança e incluam o cumprimento deste Regulamento. Estas são supervisionadas pelo Responsável de Segurança designado.
3. A informação constante do relatório da auditoria é considerada confidencial, pelo que não pode ser utilizada para outros fins sem o prévio conhecimento e a autorização do responsável do pelouro da Informática.

Artigo 29.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 30.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.
Deverão os superiores hierárquicos dar a conhecer o presente regulamento aos seus funcionários/colaboradores.

Artigo 31.º

Aprovação do Regulamento

O presente Regulamento foi aprovado pela Camara Municipal de Valpaços, no dia 19/06/2023.

Artigo 32.º

Revisão do presente regulamento

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

Artigo 33.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 34.º

Entrada em vigor

O presente Regulamento entra em vigor 5 dias após a sua publicação nos termos legais.

VERSÃO	MOTIVO DA REVISÃO	ELABORADO POR	APROVADO POR	DATA APROVAÇÃO
0.1	Criação e redação preliminar	Rosa Araújo (GI)	N/A	N/A
1.0	Redação final	Luis Chaves (DAG)	Executivo	19/06/2023