MUNICÍPIO DE VILA VERDE

AVISO

REGULAMENTO DE SEGURANÇA DO SISTEMA DE INFORMAÇÃO DO MUNICÍPIO DE VILA VERDE

Drª. Júlia Maria Caridade Rodrigues Fernandes, Presidente da Câmara Municipal de Vila Verde:

Torna Público que, nas reuniões ordinárias do Executivo, datadas de 20-12-2021 e de 07-03-2022, foi deliberado, por unanimidade, aprovar a proposta de Regulamento de Segurança do Sistema de Informação do Município de Vila Verde, bem como a alteração do mesmo.

Para constar e devidos efeitos, se publica o presente aviso e outros de igual teor, que vão ser afixados no lugar de estilo, na 2ª Série do Diário da Republica e no site do Município.

Vila Verde, 10 de março de 2022 - A Presidente da Câmara,- Drª,Júlia Maria Caridade Rodrigues Fernandes .

Regulamento de Segurança do Sistema de Informação do Município de Vila Verde

Preâmbulo

A informação, nos seus vários formatos, desempenha um papel fundamental cuja crescente importância perpassa a sociedade atual.

Para 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.

A crescente e irreversível migração da informação para um formato digital torna a sociedade, a economia, e a própria Administração Pública, cada vez mais dependentes das tecnologias de informação e de comunicação, com a vantagem, por um lado, de maiores níveis de eficácia e agilidade no tratamento e acesso, e, por outro, com o encargo de uma maior exigência ao nível da segurança, com vista a impedir o acrescido risco de eventual uso indevido.

O Município de Vila Verde procura acompanhar os avanços legislativos nacionais e europeus intentando, através 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 esteja autorizado. Para tal, com este documento estabelece-se os direitos e deveres da pessoa utilizadora do Sistema de Informação da Câmara Municipal de Vila Verde, em todas as suas componentes, digitais e físicas, definindo-se, consequentemente, a responsabilidade disciplinar e criminal, determinando, desta forma, o poder de auditoria em sede de regime disciplinar, em cumprimento das disposições legais aplicáveis, relativas à criminalidade informática, à proteção de dados pessoais e ao regime jurídico da segurança no ciberespaço.

CAPÍTULO I - DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto do Regulamento

O presente Regulamento objetiva garantir os níveis adequados de integridade, disponibilidade e confidencialidade para o sistema de informação do Município de Vila Verde, mitigando, assim, o impacto de eventuais incidentes que possam comprometer o regular funcionamento da Autarquia, promovendo a salvaguarda da informação.

O cumprimento dos objetivos elencados 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 e sistemas de informação.

Artigo 2.º

Âmbito do Regulamento

1. O Regulamento de Segurança do Sistema de Informação aplica-se a todos as pessoas autorizadas a aceder e a tratar informação do Município de Vila Verde, 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 Vila Verde, independentemente do seu suporte de registo: eletrónico, papel, audiovisual ou outro.

Artigo 3.º

Definições

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;

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 não é disponibilizada ou divulgada a indivíduos, a 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 requerido por uma entidade autorizada;

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:

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;

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.

Artigo 4.º

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 serviço 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 Vila Verde deve controlar 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 - em formato físico ou 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 para todos os tipos de pessoa autorizada, em todos os sistemas e serviços.
2. O acesso a componentes do sistema de informação, dispositivos, aplicações, sistemas ou similares, é feito mediante um processo de autenticação auditável, podendo recorrer ao uso de credenciais de acesso, como nome de utilizador e palavra-passe ou equivalente, atribuídas pela Unidade de Sistemas de Informação (USI), com base em proposta do respetivo dirigente.
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.

Responsabilidades - Dirigentes

1. A/O dirigente que superintende cada pessoa autorizada, ou dirigentes dos serviços utilizadores dos recursos, ou a/o Presidente da Câmara, ou as/os Vereadora/e(s) com competência delegada, definem as correspondentes necessidades de acesso às componentes do sistema de informação, bem como o correspondente perfil de permissões, sendo a respetiva necessidade comunicada via documento dedicado à USI ou à pessoa responsável pelo recurso do sistema de informação.

Responsabilidades – Unidade de Sistemas de Informação

1. A Unidade de Sistemas de Informação (USI) é a unidade organizacional responsável pela criação das contas de acesso com base na informação transmitida pelo dirigente.
2. Em caso de atribuição de níveis de permissão elevados, a USI pode solicitar a sua fundamentação ao dirigente responsável pela comunicação da criação de conta.
3. A USI mantém uma listagem atualizada de contas de acesso das componentes de caráter digital do sistema de informação Municipal que recorram a meios de autenticação por palavra passe ou equivalente.
4. A USI designa um número suficiente de recursos com responsabilidade de gestão de acessos privilegiados de administração de rede.
5. As funções de administrador de rede são ratificadas pela/o Presidente de Câmara.
6. A USI envia, com periodicidade semestral, a lista de contas de acesso para a Divisão de Recursos Humanos (DRH), a fim de que esta verifique possíveis alterações no perfil de competências ou outras alterações do foro laboral.
7. Os acessos a partir de localizações externas ao sistema de informação do Município são feitos mediante autorização da USI e através de recursos disponibilizados pela USI.

Responsabilidades – Divisão de Recursos Humanos

1. A Divisão de Recursos Humanos comunica à USI a cessação da relação laboral ou a transferência do/a trabalhador/a para outro serviço, secção ou unidade, a fim de que a USI possa proceder às diligências necessárias para a suspensão, cancelamento ou adequação dos acessos existentes, bem como à recolha de equipamentos ou implementação de ações de manutenção, salvaguardando informações de caráter 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 de sua responsabilidade e autoria, disponibilizando o Município, sempre que possível, redes abertas para uso pessoal.
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 receber informação 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 Vila Verde.
        ii. O Município cessa eventual tratamento de dados pessoais, caso não apresente razões imperiosas e legítimas para o mesmo sobre o qual 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. As pessoas autorizadas são responsáveis pelo correio eletrónico originado a partir de contas de *email* para as quais têm autorização de uso.
3. As pessoas autorizadas devem respeitar as proibições constantes do artigo seguinte, ou estabelecidas em quaisquer outros preceitos do presente Regulamento.
4. As pessoas autorizadas devem 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 senha, palavras do dicionário, datas, ou outras facilmente associáveis à pessoa autorizada;

b. Manter as senhas confidenciais, guardar as mesmas em *software* dedicado ou ficheiros cifrados com acesso restrito;
c. Não manter as senhas escritas em papéis ou locais visíveis;
d. Mudar as senhas regularmente, seguindo as orientações do Unidade de Sistemas de Informação;
e. Não gravar senhas de forma automática em aplicações acessíveis a partir de computadores partilhados;
f. As senhas de determinado sistema informático não devem ser reutilizadas em sistemas de diferente âmbito, mesmo que em contexto de trabalho no Município;
g. Excetuam-se da alínea anterior, as senhas de utilização múltipla usadas em mecanismos de *single sign on* (serviços de autenticação que conectam a pessoa autorizada em várias aplicações);
h. Não reutilizar *passwords* em uso em sistemas do Município em contextos de uso pessoal;

Artigo 9.º

Proibições relacionadas 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, imediatamente, ao seu superior hierárquico, bem como à USI, em caso de suspeita de uso indevido.
3. A pessoa autorizada não deve partilhar os seus privilégios de acesso com terceiros, caso tal ocorra é considerado o único responsável pelo uso dos mesmos.
4. A pessoa autorizada não deve tentar acessos não autorizados.
5. A pessoa autorizada não deve usar recursos informáticos para fins não relacionados com a missão dos serviços.

Artigo 10.º

Proibições 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 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, em circunstância alguma, proceder à ligação de novos equipamentos à rede informática sem prévio conhecimento e autorização da USI.

4. A pessoa autorizada não pode utilizar estes mesmos recursos informáticos para fins comerciais não relacionados com o Município.
5. A pessoa autorizada não pode instalar aplicações, *software* ou similar, nem alterar a configuração das aplicações ou sistemas instalados, sem autorização prévia do USI.
6. A pessoa autorizada não pode realocar dispositivos ou equipamentos informáticos.
7. A pessoa autorizada não pode recorrer a dispositivos externos para armazenamento ou qualquer outro tipo de processamento de informação, salvo se autorizado e sujeito a mecanismo de cifra que proteja os dados em caso de extravio.

SECÇÃO I - DO CORREIO ELETRÓNICO (E-MAIL)

Artigo 11.º

Responsabilidades

1. A Unidade de Sistemas de Informação é responsável pela gestão da infraestrutura de correio eletrónico, incluindo a implementação dos processos de criação e acesso a caixas de correio eletrónico.
2. A Unidade de Sistemas de Informação, conjuntamente com outras unidades organizacionais/encarregado/a de proteção de dados, 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 inferior a 30 dias e não superior a 45 dias, sendo a pessoa autorizada notificada, por escrito, pela Divisão de Recursos Humanos, devendo a pessoa autorizada que termina funções 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. Deve ser privilegiado 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 de serviço ou em mobilidade, ambas as situações num serviço externo ao município, devem permanecer inativas durante o período da comissão ou mobilidade, salvo indicação dada por escrito da/o Presidente de Câmara ou Vereador/a com o pelouro dos Recursos Humanos.
6. A Divisão de Recursos Humanos deve informar a USI num período máximo de 30 dias sobre o sobre o início da comissão de serviço ou mobilidade a que se refere o número anterior.

Artigo 12.º

Condicionantes à utilização do correio eletrónico (e-mail)

1. O uso do sistema de correio eletrónico institucional deve seguir os princípios gerais condizentes com o Código de Ética e Conduta do Município de Vila Verde.
2. São interditos na utilização de correio eletrónico os seguintes procedimentos:
    a. Falsificar mensagens de correio eletrónico;
    b. Usar o endereço de *email* 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 *email* do Município de Vila Verde 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

Acesso ao 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, à USI, sendo restrita à criação, suspensão, eliminação e gestão de atributos gerais do serviço de correio eletrónico.
2. O disposto no preceito anterior não pode pôr em causa o disposto na lei sobre direitos, liberdades e garantias da pessoa autorizada.

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 Vila Verde colaboram são princípios fundamentais, devendo para isso as pessoas autorizadas:
    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 de Vila Verde;

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 caráter institucional ou profissional em locais públicos ou privados sem garantia de reserva de privacidade;

d. Não enviar dados do Município em suporte digital para serviços em *cloud* pública, ou plataformas de uso similar geridas através de contas de acesso não controladas pelo Município.

SECÇÃO III - DO USO DE REPOSITÓRIOS

Artigo 15.º

Responsabilidades

1. O Município deve promover a implementação de repositórios digitais centralizados, que permitam o controlo de acessos com base na definição de permissões por pessoa autorizada, devendo existir repositórios partilhados por unidade organizacional e, sempre que se justifique, repositórios de acesso individual.
2. A USI é responsável pela criação, gestão, atribuição de acessos e manutenção de repositórios digitais.
3. A USI 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

Repositórios digitais

1. A pessoa autorizada deve usar os repositórios digitais (diretorias) atribuídas a cada Divisão, Serviço ou Unidade e/ou pessoa autorizada, sewndo apenas sobre os mesmos garantida a aplicação do procedimento de *backup* em vigor.
2. A pessoa autorizada a usar dispositivos com capacidade de armazenamento de dados em formato digital deve entregar o equipamento em fim de uso à USI, para que seja efetuado um procedimento de remoção de dados.
3. Os repositórios de acesso individual não devem ser usados para arquivo de dados não respeitantes à atividade do Município.

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

Artigo 17.º

Condicionantes quanto ao espaço de trabalho

1. A pessoa autorizada do sistema de informação deve seguir os princípios da mesa limpa e do ecrã limpo.
2. Os espaços de trabalho devem ser organizados por forma a prevenir a ocorrência de violações de segurança que impliquem perdas, acessos ou alterações não autorizados, quer a informação em formato físico quer em formato digital.
3. Os documentos que são transportados para trabalhar fora dos espaços físicos do Município de Vila Verde, quando autorizados, devem estar protegidos contra acesso indevido.
4. As impressões devem ser recolhidas da impressora, tão rápido quando possível, e caso se imprima documentos confidenciais deve-se acompanhar, presencialmente a saídas das folhas e garantir que foram todas recolhidas da impressora, devendo ser privilegiado o uso de código de ativação de impressão, quando tecnicamente possível.
5. A destruição de documentos em suporte físico deve ser feita com recurso a meios adequados que impossibilitem a reconstituição de documentos.

Artigo 18.º

Proibições relativas às pessoas autorizadas

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 superiormente, ou quando tal registo não decorra, diretamente, de competências atribuídas em sede de Regulamento de Organização de Serviços Municipais.
2. O uso de sistemas de impressão e digitalização está restrito a trabalhador/a(s) ou outros agentes com relação contratual com o Município.

CAPÍTULO IV – SEGURANÇA E MONITORIZAÇÃO

Artigo 19.°

Regime Jurídico da Segurança no Ciberespaço

1. O Município deve garantir a disponibilização de recursos adequados ao cumprimento das obrigações legais decorrentes do Regime Jurídico da Segurança no Ciberespaço.
2. O Município deve designar, pelo menos, um ponto de contacto permanente com o Centro Nacional de Cibersegurança 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. A USI e a Divisão de Recursos Humanos devem, conjuntamente, definir e promover 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 20.°

Deveres da Unidade Sistemas de Informação

1. Compete à USI:
    a. Manter um inventário de todos os ativos digitais essenciais para a prestação dos serviços do Município;
    b. Definir um plano de segurança baseado em análise de risco efetuada sobre os ativos essenciais que garanta a segurança dos ativos e dos dados;
    c. Detetar, mitigar e notificar incidentes de segurança nos termos do quadro legal vigente, como o Regime Jurídico da Segurança do Ciberespaço e o Regulamento Geral Sobre a Proteção de Dados;
    d. Manter no Município um registo de ocorrências de violação dos Regulamentos;
    e. Controlar o acesso físico aos equipamentos informáticos que estão sob sua gestão direta;
    f. Aplicar e manter um processo de realização de cópias de segurança e verificar, periodicamente, a sua integridade;
    g. Verificar os *logins,* acessos e registos de auditoria dos sistemas para controlar tentativas de violação e quebras de segurança;
    h. Criar e preservar registos de incidentes de segurança e fazer a sua notificação às autoridades competentes, caso necessário, nos termos do Regime Jurídico da Segurança no Ciberespaço;
    i. Acompanhar as orientações técnicas e alertas de segurança emitidos pelo Centro Nacional de Cibersegurança.

Artigo 21.º

Monitorização e criação de registos

1. **Monitorização do tráfego de rede**
    a. A USI 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. A USI 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. A USI deve, sempre que possível, privilegiar o recurso a instrumentos de monitorização que permitam a ativação de funcionalidades de pseudonimização de *logs*.
d. O acesso aos dados resultantes de processos de monitorização só pode ser concretizado com recurso a contas de acesso nominais ou de identificação unívoca.
e. 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, e operações efetuadas, devendo os *logs*, sempre que possível, ser assinados digitalmente.

2. **Arquivo de registos**
    a. A USI é responsável pelo armazenamento 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*) devem ser arquivados durante o período legalmente previsto.

Artigo 22.º

Apoio técnico

Solicitações das pessoas autorizadas à USI

1. A USI atua de forma autónoma, ou de forma articulada, com fornecedores externos, para ultrapassar quaisquer condições que se considerem anómalas na utilização dos sistemas informáticos, nos termos seguintes:
    a. A comunicação preferencial com a USI para efeitos de apoio - *helpdesk* informático - deve ser feita por via eletrónica através de preenchimento do formulário eletrónico próprio, disponível na *intranet*;
    b. O procedimento a que se refere a alínea anterior dá origem a um registo eletrónico que servirá de suporte na resposta ao pedido e para controlo interno;
    c. Os pedidos de assistência são, sempre que possível, realizados por acesso remoto, estando os recursos da USI 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 autorizada se encontra paralisado por força de problema no sistema informático ou, ainda, quando esteja em causa a segurança do sistema informático.

Artigo 23.°

Responsabilidade pela segurança e incidentes

1. As pessoas autorizadas do sistema têm 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 pelo presente Regulamento, deve ser comunicado ao superior hierárquico.

Artigo 24.°

Incidentes e suas consequências

1. Os incidentes de segurança relacionados com a componente digital do sistema de informação devem ser comunicados à/ao responsável pela segurança previsto no artigo 19.º, deste Regulamento, competindo-lhe diligenciar pela mitigação do incidente, pelo registo de evidencias e subsequente comunicação ao/à Vereador/a do Pelouro.
2. Os incidentes de segurança relacionados com a componente física do sistema de informação devem ser comunicados, respetivamente:

    a. À/Ao responsável da Divisão de Ambiente e Obras, no que concerne ao Edifício Sede e ao Edifício Principal do Parque de Máquinas;
    b. À/Ao responsável da Divisão de Educação e Promoção Social, no que concerne ao Edifício da Ação Social, Biblioteca, Complexo Desportivo de Vila Verde, Piscinas Municipais de Prado, GIP de Prado e Biblioteca de Prado;
    c. À/Ao responsável da Divisão de Águas e Saneamento no que respeita ao Armazém do Serviço de Abastecimento de Água e Saneamento;
    d. À/Ao responsável da Divisão de Qualidade Atendimento e Fiscalização, no que respeita ao Espaço Cidadão de Prado;
    e. À/Ao responsável da Unidade de Inovação e Conhecimento no que respeita ao edifício da Casa do Conhecimento.
3. As unidades orgânicas identificadas no número que antecede são responsáveis pela mitigação de incidentes, pelo registo de evidências e subsequente comunicação ao/à Vereador/a do respetivo Pelouro.

CAPÍTULO V - AUDITORIA E REGIME DISCIPLINAR

Artigo 25.º

Auditoria

1. O cumprimento deste Regulamento, no que respeita à componente de infraestrutura digital, incluindo a atividade realizada pelas pessoas autorizadas

nos equipamentos informáticos do Município pode, em qualquer altura, ser objeto de auditoria pela USI, 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 de informação e comunicação.

2. As auditorias são realizadas pela USI a pedido da/o responsável do Pelouro.
3. A informação constante do relatório da auditoria não pode ser utilizada para outros fins sem o prévio conhecimento da pessoa autorizada e a autorização do/a responsável do Pelouro da Modernização Administrativa e Sistemas de Informação e Comunicação.

Artigo 26.º

Regime disciplinar

O não cumprimento das normas do presente Regulamento determina 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 27.º

Procedimento, comunicação e localização do Regulamento

O presente Regulamento Interno deverá ser publicitado nos termos da Lei.

Artigo 28.º

Revogação

O presente Regulamento revoga o Regulamento de Utilização dos Recursos Computacionais, Rede de Dados e da Gestão de Tecnologias de Informação.

Artigo 29.º

Dúvidas e omissões

As dúvidas e omissões do presente regulamento são resolvidas por recurso à interpretação da legislação habilitante, com base em critérios de equidade, mediante decisão da/o Presidente da Câmara Municipal de Vila Verde.

Artigo 30.º

Entrada em vigor

O presente Regulamento entre em vigor 20 dias após a publicação da deliberação de aprovação.