Edital N.º: 3582
Data de registo: 31/07/2020
Assunto: Regulamento Municipal de Segurança da Informação

Célia Margarida Gomes Marques, Presidente da Câmara Municipal de Alvaiázere, torna público, ao abrigo da competência que lhe é conferida pela alínea t) do n.º 1 do artigo 35.º do Anexo I da Lei n.º 75/2013, de 12 de Setembro, que, por deliberação da Câmara Municipal de Alvaiázere tomada na sua reunião ordinária de 17 de julho de 2020, foi aprovado o projeto de "Regulamento Municipal de Segurança da Informação", tendo por base o artigo 241º da Constituição da República Portuguesa e a alínea g) do nº 1 do artigo 25º e a alínea k) do n.º 1 do artigo 33º da Lei nº 75/2013, de 12 de setembro.----------

Assim, nos termos e para efeitos do disposto no artigo 12.º, da alínea c) do n.º 3 do artigo 100.º e no artigo 101.º do Código do Procedimento Administrativo, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, submete-se o referido projeto de "Regulamento Municipal de Segurança da Informação" a consulta pública, pelo prazo de 30 dias úteis contados a partir da data da publicação do presente aviso na 2.ª série do Diário da República.----------

O referido projeto encontra-se disponível para consulta na Subunidade Orgânica da Apoio ao Munícipe e Tesouraria desta Câmara Municipal, a funcionar na Loja do Cidadão, bem como no *site* do Município de Alvaiázere na internet (www.cm-alvaiazere.pt).----------

As sugestões, propostas e/ou reclamações deverão ser apresentadas, por escrito, no prazo de 30 dias úteis a contar da data da publicação deste aviso no Diário da República, devendo ser dirigidas à Presidente da Câmara Municipal de Alvaiázere, por via postal, para a Praça do Município, 3250-100 Alvaiázere, entregues pessoalmente nos serviços de atendimento do Município (Subunidade Orgânica de Apoio ao Munícipe e Tesouraria) ou por correio electrónico para: geral@cm-alvaiazere.pt., com a identificação do remetente, morada e identificação fiscal, até ao último dia do prazo supra referido.----------

Para constar e devidos efeitos, se publica o presente edital e outros de igual teor, que vão ser afixados nos lugares públicos do costume.

Alvaiázere, 31/07/2020

A Presidente da Câmara Municipal,

CÉLIA MARGARIDA GOMES MARQUES
Digitally signed by CÉLIA MARGARIDA GOMES MARQUES
Date: 2020.07.31 11:37:42 +01:00
Location: Portugal

Célia Margarida Gomes Marques

MUNICÍPIO DE ALVAIÁZERE

Edital n.º 911/2020

Sumário: Regulamento Municipal de Segurança da Informação — consulta pública.

Célia Margarida Gomes Marques, Presidente da Câmara Municipal de Alvaiázere, torna público, ao abrigo da competência que lhe é conferida pela alínea *t*) do n.º 1 do artigo 35.º do Anexo I da Lei n.º 75/2013, de 12 de setembro, que, por deliberação da Câmara Municipal de Alvaiázere tomada na sua reunião ordinária de 17 de julho de 2020, foi aprovado o projeto de "Regulamento Municipal de Segurança da Informação", tendo por base o artigo 241.º da Constituição da República Portuguesa e a alínea *g*) do n.º 1 do artigo 25.º e a alínea *k*) do n.º 1 do artigo 33.º da Lei n.º 75/2013, de 12 de setembro.

Assim, nos termos e para efeitos do disposto no artigo 12.º, da alínea *c*) do n.º 3 do artigo 100.º e no artigo 101.º do Código do Procedimento Administrativo, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, submete-se o referido projeto de "Regulamento Municipal de Segurança da Informação" a consulta pública, pelo prazo de 30 dias úteis contados a partir da data da publicação do presente aviso na 2.ª série do *Diário da República.*

O referido projeto encontra-se disponível para consulta na Subunidade Orgânica da Apoio ao Munícipe e Tesouraria desta Câmara Municipal, a funcionar na Loja do Cidadão, bem como no *site* do Município de Alvaiázere na internet (www.cm-alvaiazere.pt).

As sugestões, propostas e/ou reclamações, deverão ser apresentadas, por escrito, no prazo de 30 dias úteis a contar da data da publicação deste aviso no *Diário da República,* devendo ser dirigidas à Presidente da Câmara Municipal de Alvaiázere, por via postal, para a Praça do Município, 3250-100 Alvaiázere, entregues pessoalmente nos serviços de atendimento do Município (Subunidade Orgânica de Apoio ao Munícipe e Tesouraria) ou por correio eletrónico para: geral@cm-alvaiazere.pt., com a identificação do remetente, morada e identificação fiscal, até ao último dia do prazo supra referido. Para constar e devidos efeitos, se publica o presente edital e outros de igual teor, que vão ser afixados nos lugares públicos do costume.

31 de julho de 2020. — A Presidente da Câmara, *Célia Margarida Gomes Marques*.

313458112

Divisão Administrativa e Financeira

Tecnologias da Informação

Regulamento de Segurança da Informação

Município de alvaiázere

Sorte em viver aqui.

Criado por:	Serviço de Tecnologias da Informação (TI)
Aprovado por:	Presidente da Câmara
Versão:	[Keywords]
Data da versão:	10/07/2020
Nível de confidencialidade:	[Status]

Controlo e Aprovação do Documento

Controlo do Documento

Responsável	Serviço de Tecnologias de Informação (TI)

Histórico de Alterações

Versão	Data	Autor	Descrição das alterações
1.0	10/07/2020	TI	Elaboração do documento

Aprovação do Documento

Elaboração: Chief Security Officers, S.A.	Verificação: Célia Ferreira	Aprovação: Célia Marques
Cargo: Data: 10/07/2020	Cargo: Chefe de Divisão Data: 10/07/2020	Cargo: Presidente da Câmara Data: 10/07/2020

Índice

Nota Justificativa

A Lei n.º 46/2018, de 13 de agosto, estabelece o regime jurídico da segurança no ciberespaço, transpondo a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação.

O ciberespaço facilita muitas das tarefas a desenvolver pelo Município de Alvaiázere; contudo, a interligação das redes e dos sistemas de informação e de comunicação torna os serviços vulneráveis às ameaças inerentes a este espaço virtual. A rede digital, atenta a sua natureza transfronteiriça, é caracterizada pela ausência de limites territoriais e físicos, oferecendo uma realidade que carece do equacionamento de novas questões de segurança. Neste contexto, a Lei n.º 46/2018, anteriormente referida, estabelece um regime jurídico da segurança no ciberespaço para todas as entidades que utilizem sistemas e redes de informação, sendo aplicável, nomeadamente, às autarquias locais, incumbindo-as de regulamentar neste âmbito.

A necessidade da implementação de políticas e procedimentos de segurança resulta do dever dos órgãos e serviços da Administração Pública de utilizarem os meios eletrónicos no desempenho da sua atividade de forma a garantirem a disponibilidade, o acesso, a integridade, a autenticidade, a confidencialidade a conservação e a segurança da informação, dever este plasmado no artigo 14º do Código do Procedimento Administrativo.

Destarte, cabe ao Município de Alvaiázere definir as medidas técnicas e organizativas adequadas e proporcionais, de modo a gerir os riscos que se colocam à segurança das redes e dos sistemas de informação utilizados, devendo, estas, garantir um nível de segurança adequado ao risco e evitar incidentes.

A segurança da informação é obtida através da implementação de um conjunto de controlos, que necessitam de ser estabelecidos para assegurar que objetivos específicos de segurança de informação sejam atingidos, tendo por base a norma internacional ISO 27002, criada para apontar as normas necessárias para uma segurança de informação mais eficiente para as organizações. O foco encontra-se, assim, em determinar quais os princípios para iniciar, implementar, manter e melhorar a gestão de segurança de informação. Esta norma define o código de boas práticas, encontrando-se as medidas sugeridas na presente proposta de regulamento de acordo com ela.

Com efeito, com a presente proposta de regulamento pretende-se, assim, definir a Política de Segurança de Informação: a estratégia e as normas que devem ser aplicadas no âmbito da gestão de segurança de informação, traduzindo as normas uma *framework* de controlos que devem ser executados ao nível dos processos e procedimentos, e proceder ao relato regular e transparente do seu desempenho na matéria da segurança de informação, de forma a reduzir os riscos, garantindo e reforçando a conformidade com a regulamentação e as exigências legais em vigor. Assim, algumas das principais vantagens deste processo de implementação podem ser resumidas da seguinte forma:

1. um maior respeito, por parte do mercado, munícipes e parceiros, garantindo um maior crédito na função de segurança da informação;
2. a demonstração de apoio efetivo e evidente da gestão de topo para o tema da segurança de informação;
3. o estabelecimento de canais de comunicação formais entre os níveis de decisão e gestão.

Resulta, desta forma, que a aprovação da presente proposta de regulamento se prefigura como necessária para garantir a integridade, a confidencialidade, a disponibilidade, a rastreabilidade, a conformidade legal e a auditabilidade da informação, servindo de base a um sistema de gestão e organização de segurança de informação.

Preâmbulo

Decorrido o procedimento de elaboração previsto na lei, sob proposta da Câmara Municipal, a Assembleia Municipal de Alvaiázere aprova, sob a forma de regulamento, o Regulamento Municipal de Segurança de Informação, nos termos da alínea g) do n.º 1 do artigo 25.º e da alínea k) do n.º 1 do artigo 33.º da Lei n.º 75/2013, de 12 de setembro, cujo Projeto foi publicado pelo Aviso n.º ____/____, do Município de Alvaiázere, na 2.ª série do Diário da República n.º __, de __ de _____ de 2020, disponibilizado na Subunidade Orgânica de Apoio ao Munícipe e Tesouraria na Loja do Cidadão e na página eletrónica do Município de Alvaiázere, em www.cm-alvaiazere.pt, com vista à sua consulta pública por 30 dias.

CAPÍTULO I - Disposições Gerais

Artigo 1.º - Lei Habilitante

O presente Regulamento é elaborado ao abrigo do disposto no artigo 241.º da Constituição da República Portuguesa, da alínea k) do n.º 1 do artigo 33.º do Anexo I da Lei n.º 75/2013, de 12 de setembro, na sua redação atual, que aprova o Regime Jurídico das Autarquias Locais, das Entidades Intermunicipais e do Associativismo Autárquico e do artigo 14º da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança no ciberespaço, conjugado com o artigo 14º do Código do Procedimento Administrativo, na sua redação atual.

Artigo 2.º - Objeto e âmbito de aplicação

1. O presente regulamento define as políticas e procedimentos de segurança de informação e de controlo de riscos a implementar pelo Município de Alvaiázere;
2. Estas políticas e todas as normas e procedimentos que dela derivam abrangem a totalidade da informação gerida, independentemente do seu suporte ou via de transmissão;
3. As disposições do presente regulamento são aplicáveis a todos órgãos, serviços e organismos municipais do Município de Alvaiázere, às entidades externas que exerçam competências municipais em regime de delegação de competências e às demais entidades externas relevantes.

Artigo 3.º - Siglas

Para efeitos deste regulamento, utilizam-se as seguintes siglas:

CISO: *Chief Information Security Officer;*
COM: *Computer Operations Manager;*
CSI: Comissão de Segurança da Informação;
DRH: Direção de Recursos Humanos;
GAI: Gabinete de Auditoria Interna;
IEC: *International Electrotechnical Commission;*
ISO: *International Standards Organization;*
PDCA: Plan (planear), Do (executar), Check (verificar), Act (agir);
SGSI: Sistema de Gestão de Segurança de Informação;
SI: Sistemas de Informação
SISA: *Senior Information Security Advisor;*
SHORE: Subunidade Orgânica de Recursos Humanos e Expediente;

TCO: *Total Cost of Ownership*
TI: Tecnologias de Informação
VPN: *Virtual Private Network*

Artigo 4.º - Definições

Consideram-se, para efeitos deste regulamento, as seguintes definições:

a) *BitLocker*: sistema de criptografia do Windows, presente em versões do Windows 7, Windows 8 e no Windows 10. Encripta partições dos dispositivos de armazenamento, protegendo os documentos e ficheiros contra o acesso não autorizado;
b) *Colaborador*: trabalhadores com contrato de trabalho com o Município, trabalhadores temporários ou consultores;
c) *Download*: obtenção de dados de um dispositivo através de um canal de comunicação;
d) *Entidade externa*: pessoas/munícipes ou entidades que não sejam colaboradores, trabalhadores temporários ou consultores do Município de Alvaiázere;
e) *Fornecedor*: aqueles que fornecem bens e serviços considerados no âmbito do Sistema de Gestão de Segurança de Informação (SGSI);
f) *Framework*: conjunto de elementos e das suas interligações constituindo a base de um sistema ou projeto;
g) *Gateway*: ou "porta de ligação", em informática é um dispositivo intermediário, geralmente destinado a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos;
h) Incidente de segurança: violação ou ameaça eminente à Política de Segurança de Informação do Município de Alvaiázere. São incidentes de segurança, entre outros, o acesso, tentativa de acesso, uso, divulgação, modificação ou destruição não autorizada de informação, ou ainda o impedimento do funcionamento normal das redes, sistemas ou recursos informáticos;
i) Informação: todo e qualquer dado, de qualquer natureza, incluindo dados relativos à atividade do Município de Alvaiázere, ou de terceiros com quem se relacione, que a organização coloque à disposição dos seus colaboradores e de entidades externas, ou de que estes possam vir a ter conhecimento ou acesso no exercício das suas funções;
j) *Password*: informação secreta utilizada para controlar o acesso a um recurso. É geralmente utilizada em conjunto com a identificação do utilizador em mecanismo de autenticação;
k) Perfil de Acesso: conjunto de privilégios permitidos entre um utilizador e um recurso considerando as políticas de fluxo de informação definidas;
l) Privilégios: ação que um perfil de acesso pode realizar sobre os ativos de informação;
m) Proxy: equipamento que funciona como intermediário entre um *web browser* (tal como o Internet Explorer) e a Internet, melhorando o desempenho no acesso a páginas *web*;
n) *Streaming*: forma de distribuição de dados, geralmente de multimédia, numa rede, através de pacotes. É frequentemente utilizada para distribuir conteúdo multimédia através da Internet;
o) *Upload*: transferência de dados de um computador local para outro computador ou para um servidor;
p) VPN: rede de comunicações privada construída sobre uma rede de comunicações pública (como, por exemplo, a Internet).

CAPÍTULO II - Política de Segurança de Informação

SECÇÃO I - A Política de Segurança de Informação

Artigo 5.º - Objetivos gerais da Política de Segurança de Informação

A Política de Segurança a implementar tem como principal objetivo o estabelecimento dos pilares de Segurança dos Sistemas de Informação, de modo a assegurar:

a) A acessibilidade controlada e a disponibilidade dos sistemas, de acordo com a criticidade e o valor da informação por eles processada;
b) A confidencialidade, integridade e disponibilidade da informação em qualquer suporte;
c) A rastreabilidade e a conformidade legal;
d) A continuidade das operações.

Artigo 6.º - Comunicação

1. As políticas, normas e procedimentos relativos à segurança de informação devem ser de conhecimento obrigatório dos colaboradores e das entidades externas relevantes, independentemente do seu vínculo contratual com o Município de Alvaiázere;
2. É da responsabilidade do Município de Alvaiázere a divulgação da Política de Segurança de Informação junto dos seus colaboradores e das entidades externas, enquanto seus prestadores de serviços;
3. Para efeitos dos números anteriores, cabe, igualmente, ao município garantir a sua aceitação e cumprimento por todos, e implementar ações de formação e de sensibilização adequadas.

Artigo 7.º - Divisões e Serviços do Município

1. As divisões e serviços do Município de Alvaiázere são responsáveis por garantir e manter as políticas, normas e controlos de segurança de informação definidos pela respetiva direção;
2. Para efeitos do número anterior, devem implementar e monitorizar controlos tecnológicos, fixados pela respetiva direção, de forma a garantir a integridade, disponibilidade e confidencialidade da informação;
3. São, também, responsáveis por colaborarem ativamente com a Comissão de Segurança de Informação no tratamento de assuntos no âmbito da segurança de informação.

Artigo 8.º - Colaboradores, entidades externas e fornecedores

1. Todos os colaboradores do Município de Alvaiázere e entidades externas com acesso à informação são responsáveis pela sua proteção;
2. Consultores externos, colaboradores contratados e trabalhadores temporários estão sujeitos aos mesmos requisitos de segurança e têm as mesmas responsabilidades no cumprimento dos requisitos de segurança da informação do Município de Alvaiázere;
3. Todos os parceiros de serviço, fornecedores e clientes do Município de Alvaiázere devem ser sensibilizados para as responsabilidades de cumprimento da política de segurança de informação, através de comunicação específica presente nos contratos que definem a sua relação com o município.

SECÇÃO II - Comissão de Segurança de Informação

Artigo 9.º - Comissão de Segurança de Informação

A Comissão de Segurança de Informação, doravante CSI, é a estrutura funcional responsável pela segurança de informação do Município de Alvaiázere.

Artigo 10.º - Âmbito de atuação

1. A CSI define e implementa uma estratégia de segurança de informação através:
   a) do estabelecimento e implementação de um sistema de gestão de segurança de informação e do controlo do mesmo, através de métricas contínuas de avaliação interna;
   b) da aprovação e implementação dos documentos (normas, procedimentos e políticas) relacionados com o Sistema de Gestão de Segurança de Informação cujo conteúdo caiba no âmbito das atuais competências do serviço de Tecnologias da Informação;
2. Os restantes documentos não mencionados na alínea b) do número anterior são apresentados e analisados previamente pelos serviços jurídicos, que avaliam a sua conformidade com a legislação em vigor e com os regulamentos internos da entidade, bem como a necessidade destes serem aprovados pelo Município de Alvaiázere.

Artigo 11.º - Estrutura

A CSI é composta por:

a) Presidente da Comissão de Segurança;
b) Vice-Presidente da Comissão de Segurança;
c) *Computer Operations Manager* (COM);
d) Gabinete de Auditoria Interna (GAI);
e) *Senior Information Security Advisor* (SISA).

Artigo 12.º - Presidente da Comissão de Segurança

1. O Presidente da Comissão de Segurança (*Chief Information Security Officer* – CISO) dirige, planeia e organiza as atividades associadas à disciplina de segurança da informação internamente;
2. É da responsabilidade do Presidente da CSI:

   a) estabelecer e manter um relacionamento de funcionamento forte com as equipas envolvidas no tema da segurança de informação;
   b) apoiar no esclarecimento da responsabilidade individual de cada colaborador, de modo a que as atividades e procedimentos de segurança sejam executados como previsto e acordado nas decisões de segurança e políticas do município;
   c) coordenar todos os projetos de evolução de segurança aplicacional ou atualização aplicacional no âmbito do sistema de segurança de informação;
   d) desenvolver os planos de ação, planeamento, orçamentos associados, relatórios de avaliação e outros documentos de *reporting* para a Câmara Municipal, de forma a melhorar o nível de segurança de informação;
   e) obter aprovação da Câmara Municipal e o respetivo suporte para todas as iniciativas principais da segurança de informação;
   f) gerir as vulnerabilidades de segurança existentes nos sistemas de informação de forma a garantir a atenção e sensibilidade da Câmara Municipal, no intuito de acionar as medidas corretivas em tempo útil;

g) controlar o desempenho das auditorias periódicas de segurança e de risco na entidade que identifica as vulnerabilidades de segurança, atuais e futuras, permitindo determinar qual o nível do risco aceitável para a entidade, e identificar as melhores formas de reduzir os riscos da segurança a um nível considerado como aceitável para a gestão de topo;
h) assistir no estabelecimento e refinamento dos procedimentos para a identificação de recursos de informação da entidade, tal como a classificação desses recursos no que respeita ao nível de criticidade, ameaça, vulnerabilidade, impacto e valor;
i) definir e controlar os processos para a deteção, investigação, correção, propor ação disciplinar associada, e/ou a pesquisa e investigação relacionada com falhas e incidentes de segurança de informação e posterior comunicação à Câmara Municipal;
j) dirigir a preparação dos planos de contingência do sistema de informação e controlar os grupos de trabalho que respondem aos eventos relevantes de segurança de informação na entidade;
k) sensibilizar os diversos níveis da entidade para a necessidade de promover níveis elevados de qualidade no sistemas e tecnologias de informação;
l) garantir que todos os colaboradores do município têm, pelo menos uma vez por ano, ações de sensibilização e formação na área de Segurança em Sistemas de Informação;
m) organizar sessões de passagem de conhecimento para garantir a conformidade com as exigências e normas de segurança de informação internamente.

Artigo 13.º - Gabinete de Auditoria Interna

O Gabinete de Auditoria Interna (GAI) é responsável por:

a) fornecer um relatório do controlo interno, bem como a sua avaliação;
b) participar na documentação de incidentes de segurança de informação junto das autoridades e do Presidente da Comissão de Segurança;
c) atuar como controlador interno no que respeita as indicações das exigências/requisitos, de análises da praticabilidade, de manuais de procedimentos e de outros documentos produzidos durante o processo de desenvolvimento dos sistemas;
d) assistir ao esforço interno desenvolvido pela equipa de sistemas de informação e comunicação no processo de inventário e controlo da propriedade intelectual;
e) acompanhar no desenvolvimento anual do modelo de classificação de informação, que permita que os utilizadores decidam, em tempo útil, sobre os procedimentos a adotar na proteção da informação que lhes está atribuída.

Artigo 14.º - *Senior Information Security Advisor (SISA)*

1. O SISA é uma entidade externa de consultoria/auditoria, nomeada pelo município;
2. É responsável por:

a) fornecer o conselho técnico aprofundado para processo de investigação de incidentes da segurança de informação, incluindo fraudes, intrusões, roubo e acessos ilícitos internos e externos na entidade;
b) participar na documentação de incidentes de segurança de informação junto das autoridades e gestão de topo da entidade, apoiando também a análise das circunstâncias e envolvência técnica, permitindo mitigar e/ou bloquear esses incidentes de ocorrer no futuro imediato;
c) analisar e avaliar, a pedido, as soluções e propostas comercias relacionados com o tema da segurança de informação, no intuito de determinar qual a melhor opção a ser adotada face às necessidades detetadas;
d) fornecer sustentação técnica aos colaboradores e órgãos de gestão nas matérias relacionadas com a segurança de informação, como os critérios de avaliação na utilização/adoção de produtos de segurança de informação;

e) atuar como revisor de segurança de informação técnica no que respeita às indicações das exigências/requisitos, de análises da praticabilidade, de manuais de procedimentos, e de outros documentos produzidos durante o processo de desenvolvimento dos sistemas;
f) fornecer a orientação técnica à equipa de colaboradores e operadores do serviço de TI sobre os riscos e as medidas de controlo associadas com as novas tecnologias e ameaças emergentes dos sistemas de informação;
g) atuar enquanto recurso técnico altamente qualificado e a pedido do Presidente da Comissão de Segurança, junto dos órgãos de gestão, responsáveis dos serviços, colaboradores, ou outro qualquer elemento que necessite de informação sobre a disciplina de segurança de informação;
h) participar e agir como líder/auditor técnico durante as avaliações de risco associadas com o desenvolvimento de novas aplicações de serviço;
i) preparar e atualizar periodicamente as propostas de políticas de segurança de informação, arquiteturas TI/SI, padrões e normas, e/ou outra exigência técnica documentada e necessária para avançar a estratégia de segurança de informação na entidade;
j) interpretar as políticas de segurança de informação, padrões e normas, e/ou outras exigências no âmbito dos sistemas e tecnologias de informação internos e auxiliar a equipa de sistemas na implementação destas e outras exigências que se julguem pertinentes;
k) fornecer o conselho técnico e passagem de conhecimento aos operadores e administradores do sistema de informação;
l) assistir ao esforço interno desenvolvido pelo Serviço de TI no processo de inventário e controlo da propriedade intelectual;
m) desenvolver e refinar periodicamente o modelo de classificação de informação, que permita que os utilizadores decidam em tempo útil sobre os procedimentos a adotar na proteção da informação que lhes está atribuída;
n) monitorizar e manter-se atualizado sobre as leis atuais e propostas, regulamentos, padrões e melhores práticas da indústria e as exigências éticas que se relacionam com a disciplina de segurança de informação e a privacidade dos dados. Desta forma, a entidade tem antecipadamente acesso à informação e pode preparar-se, em tempo útil, para cumprir integralmente com as novas recomendações;
o) é responsável pelo processo formal de auditoria de segurança de informação e respetiva apresentação dos resultados à CSI.

Artigo 15.º - *Computer Operations Manager* (COM)

O COM:

a) controla, em colaboração com os serviços responsáveis pela respetiva área, a estrutura elétrica, comunicações telefónicas, ar condicionado, controlo da humidade, a deteção e a supressão de fogo e outros sistemas ambientais que são necessários para a operação contínua dos recursos associados aos sistemas de informação;
b) supervisiona o processo da gestão e controlo da alteração da plataforma de equipamentos, instalações e *software*, garantindo que somente as alterações devidamente autorizadas são efetivamente realizadas;
c) planeia e supervisiona *upgrades* de *hardware* e de *software* para os sistemas de informação controlados pelo serviço de TI, de modo a que a integridade, disponibilidade e segurança dos sistemas de informação sejam mantidos;
d) mantem um inventário atualizado do equipamento associado aos sistemas de informação;
e) promove consultoria técnica interna para auxiliar os colaboradores e utilizadores das aplicações de serviço, melhorando a utilização da plataforma tecnológica e aplicacional controlados pelo serviço de TI;
f) executa análises e avaliações de capacidade e desempenho dos equipamentos, instalações e plataformas de *software* instalados no *Datacenter*, bem como em bastidores de comunicações;

g) estabelece e supervisiona o sistema de distribuição de impressão e outro qualquer sistema de visualização de matéria considerada sensível, de forma a ser recebido e visualizado somente por utilizadores devidamente autorizados;
h) gere, controla e monitoriza todos os ativos relacionados com o TI;
i) supervisiona o trabalho de entidades terceiras quando estão residentes nas áreas de responsabilidade do serviço de TI.

Artigo 16.º - Serviço Jurídico

A CSI pode solicitar a colaboração do Gabinete de Contratação Pública, Assessoria e Fiscalização para a validação da conformidade legal da Segurança de Informação no Município de Alvaiázere.

Artigo 17.º - Serviço de Recursos Humanos

A CSI define, em colaboração com a Subunidade Orgânica de Recursos Humanos e Expediente (SOHRE), as ações a desencadear para a sensibilização dos colaboradores do Município de Alvaiázere para as questões de segurança da informação.

SECÇÃO III - Política de Organização Externa e Interna

Artigo 18.º - Organização externa

1. O serviço de TI identifica os riscos relacionados com o acesso de entidades externas à informação;
2. São entidades externas pessoas/munícipes ou entidades que não sejam colaboradores, trabalhadores temporários ou consultores do Município de Alvaiázere;
3. As entidades externas não têm acesso aos recursos de informação corporativos da organização, exceto quando previamente autorizados, de forma escrita, pelos dirigentes municipais;
4. O acesso a informação relacionada com os sistemas de informação do município pelas entidades externas apenas é autorizado se for demonstrada a existência da necessidade de conhecimento e quando seja expressamente autorizado pela CSI, sob coordenação do serviço de TI, a solicitação de um serviço;
5. Atividades que tenham como requisito o acesso a áreas críticas da informação do município apenas são realizadas se acompanhadas por um elemento da instituição, exceto em situações de emergência ou desastre que requeiram a utilização de colaboradores adicionais.

Artigo 19.º - Acordos de confidencialidade

1. Todas as entidades externas que contenham informação da organização assinam um acordo de confidencialidade com o Município de Alvaiázere, antes de serem efetuados processos de instalação, configuração, suporte, manutenção ou reparação de ativos de TI;
2. Qualquer tipo de divulgação de informação corporativa classificada como confidencial a parceiros externos é realizada através de assinatura de um acordo de confidencialidade que inclua as restrições na subsequente disseminação e uso da informação.

Artigo 20.º - Termos e condições dos acessos de parceiros externos

1. O acesso a sistemas de informação internos por parceiros externos só é possível se for autorizado pela CSI, sob coordenação do serviço de TI, a solicitação de um serviço;
2. O acesso remoto por parceiros externos só é possível quando for aprovada pela CSI a necessidade legítima desse acesso, que deve ser feito de forma controlada, a determinados recursos corporativos, a determinadas pessoas e durante um horário específico, conforme os casos;
3. Antes de ser concedido qualquer tipo de acesso aos sistemas corporativos a parceiros externos, deverá ser assinado um contrato entre ambos que defina os termos e condições do acesso à informação da instituição;
4. O contrato mencionado no número anterior é assinado por um gestor responsável do parceiro externo e aprovado pela CSI e pelo serviço que efetuou o pedido.

Artigo 21.º - Uso do nome da instituição por parceiros externos

Nenhum parceiro externo deverá utilizar o bom nome do Município de Alvaiázere para seu benefício ou em propósitos de marketing ou publicidade, exceto se obtiver autorização para tal.

Artigo 22.º - Tratamento da informação corporativa no término de contratos

1. Se o Município de Alvaiázere terminar o contrato de prestação de serviços com algum parceiro externo que tenha em sua posse informação privada da instituição, a mesma é entregue ao cuidado da organização ou destruída de imediato;
2. Após o término dos seus contratos, todos os colaboradores contratados, consultores e trabalhadores temporários cedem ao seu dirigente de serviço, toda a informação referente à instituição que esteja em sua posse e que tenha sido rececionada ou criada durante a duração do contrato.

Artigo 23.º - Organização interna

A organização interna:

a) coordena a segurança da informação;
b) aloca as responsabilidades pela segurança da informação;
c) define o processo de autorização para infraestruturas de processamento de informação;
d) faz uma revisão independente de segurança da informação;
e) identifica os riscos associados a partes externas;
f) gere a segurança de informação no Município de Alvaiázere.

Artigo 24.º - Propriedade da informação

O Presidente da CSI especifica, ao nível do inventário de ativos, a atribuição da responsabilidade pela propriedade da informação de bases de dados, ficheiros corporativos, assim como outro tipo de informação partilhada e designa os responsáveis por manter os direitos de acesso a essa informação, em alternativa aos seus proprietários.

Artigo 25.º - Promoção da segurança de informação

1. À CSI cabe garantir que a segurança da informação é encarada como um problema que deverá ser visto e resolvido, e é responsável por garantir a segurança para todas as unidades de serviço;
2. Deverão ser alocados recursos e colaboradores suficientes, de forma a tratar da melhor forma dos sistemas de segurança de informação;
3. As soluções e serviços de segurança de informação são garantidos através do orçamento do Serviço de Informática;
4. A CSI, em conjunto com a direção de sistemas de informação e comunicação, prepara, sempre que julgar necessário, planos que incrementem o nível de segurança na plataforma de serviços corporativos do Município de Alvaiázere.

Artigo 26.º - Aprovação de alterações

A CSI deve garantir que nenhuma alteração aos sistemas corporativos, solicitada ou promovida por um serviço da instituição, é efetuada sem a sua prévia autorização.

Artigo 27.º - Centralização da segurança de informação

Normas, procedimentos e boas práticas para a gestão da segurança de informação são centralizados para toda a instituição pela CSI.

Artigo 28.º - Segregação de funções

1. As funções e as áreas de responsabilidade são segregadas para reduzir as oportunidades de modificação ou uso indevido, não autorizado ou involuntário dos recursos associados à informação e à infraestrutura de processamento da informação do Município de Alvaiázere;
2. A alteração de qualquer ativo só pode ser efetuada com a autorização do respetivo dono;
3. Os controlos de segurança de informação devem ser desenhados para prevenir conluios;
4. Sempre que a segurança de informação dos ativos não possa ser controlada por segregação de deveres e responsabilidades, há uma supervisão mais rigorosa das atividades de trabalho;
5. Devem ser criados registos de auditoria e procedimentos de monitorização quando não for possível garantir a segregação indicada;
6. As auditorias de segurança de informação são independentes.

Artigo 29.º - Fórum de segurança da informação

1. É criado um comité de gestão da segurança de informação, composto por um conjunto de elementos relevantes para o Município de Alvaiázere, internos e externos, e devidamente selecionados pelo CSI;
2. O comité mencionado no número anterior tem funções operacionais de análise do estado atual das métricas da segurança de informação presentes na instituição e analisa os processos de monitorização dos incidentes de segurança ocorridos;
3. É responsabilidade do comité analisar e mais tarde aprovar os projetos relacionados com a segurança da informação, assim como analisar e aprovar políticas de segurança da informação, novas ou modificadas.

Artigo 30.º - Coordenação da informação

1. Para qualquer risco significativo relacionado com os sistemas de segurança de informação da instituição, é efetuada uma análise de aceitação de risco e são tomadas medidas específicas para esse mesmo nível de aceitação;
2. Devem ser implementadas medidas de segurança adequadas para a abrangência do risco identificado e para ameaça identificada, de forma a garantir a confidencialidade, integridade e disponibilidade da informação mantida pelos sistemas de informação e comunicação do Município de Alvaiázere.

Artigo 31.º - Controlos de novas tecnologias

1. Em todos os casos onde se possa utilizar novas tecnologias nos sistemas produtivos do Município de Alvaiázere, os controlos e operações de segurança associados a novas tecnologias devem ser particularmente rigorosos, até que as mesmas se mostrem como confiáveis e fáceis de controlar através das atividades de serviço;
2. Todos os sistemas produtivos de informação são periodicamente avaliados pela CSI, de forma a obter um conjunto de controlos de segurança a implementar para reduzir e manter o risco num nível aceitável.

Artigo 32.º - Paragem de componentes de segurança críticos

Os sistemas críticos de infraestrutura de segurança de informação do Município de Alvaiázere não devem parar, ser desligados ou desativados, sem aprovação prévia da CSI.

Artigo 34.º - Análise crítica e independente da segurança da informação

É feita uma análise externa e independente aos sistemas de informação periodicamente, de forma a se obter o resultado da sua aplicabilidade e conformidade com os controlos de segurança implementados na instituição.

CAPÍTULO III - Gestão de acessos

SECÇÃO I - Política de Gestão de Acessos

Artigo 35.º - Gestão de utilizadores e privilégios

1. O registo de utilizadores para conceder, alterar e revogar os acessos a todos os serviços e sistemas de informação realiza-se através de um procedimento formal;
2. Os colaboradores do Município de Alvaiázere e as entidades externas têm de assinar um termo de responsabilidade antes de lhes ser atribuído qualquer acesso aos sistemas;
3. O termo de responsabilidade a que alude o número 2 do presente artigo deve incluir as regras e condições definidas para o seu acesso e respetivas responsabilidades;
4. Cada sistema deve ter identificado um conjunto de perfis e privilégios, que devem ser alocados aos utilizadores conforme a necessidade;
5. Os privilégios de acesso aos sistemas são atribuídos aos colaboradores e entidades externas considerando as necessidades efetivas para o desempenho das suas funções, não devendo ser atribuídos nem por excesso nem por defeito;

6. Os privilégios de acesso aos sistemas do Município de Alvaiázere devem, por omissão, bloquear o acesso aos utilizadores não autorizados;
7. Os privilégios de acesso aos sistemas devem garantir uma correta segregação de funções ou, nos casos em que não é possível garantir a segregação de funções, deverão estar implementados os controlos compensatórios adequados;
8. Os pedidos de criação, alteração e revogação de acessos e privilégios de qualquer utilizador são dirigidos ao serviço de TI, onde serão encaminhados para um circuito de aprovação envolvendo a hierarquia e donos dos recursos;
9. Os acessos e respetivos privilégios só devem ser implementados nos sistemas depois de obtidas todas as aprovações necessárias;
10. Deve ser mantido um registo formal de todos os utilizadores autorizados e respetivos privilégios de acesso aos sistemas da organização;
11. Qualquer alteração à condição profissional dos colaboradores e entidades externas que envolva alteração das necessidades efetivas de acesso aos sistemas deve ser imediatamente refletida nos acessos e privilégios disponibilizados, por solicitação ao serviço de TI, onde serão encaminhados para um circuito de aprovação envolvendo a hierarquia e donos dos recursos;
12. Os privilégios de acesso aos sistemas disponibilizados aos colaboradores e entidades externas devem ser revogados, de forma automática, assim que terminem a sua relação profissional com o Município de Alvaiázere;
13. As contas de utilizador não usadas durante um determinado período de tempo são desativadas e/ou removidas através de um procedimento periódico de revisão, exceto nos casos em que existe uma justificação formal para manter as respetivas contas;
14. Para efeitos do número anterior, o período de tempo aceitável para uma conta poder manter-se ativa sem utilização deve ser definida por sistema, de acordo com as características do respetivo sistema.

Artigo 36.º - Identificadores (*User ID's*)

1. Os colaboradores e entidades externas têm associado, para cada sistema ao qual tenham permissões de acesso, um identificador (*user* ID) único e uma *password* intransmissível;
2. A utilização de identificadores genéricos (contas genéricas ou de grupo) deve ser permitida apenas quando o sistema não permita efetuar uma gestão de utilizadores individuais, tendo esta utilização de ser aprovada pelo responsável da área e documentada, e devem ter um período de existência que seja o necessário e suficiente para a execução da tarefa em causa;
3. Cada conta genérica tem associado um utilizador individual responsável por essa mesma conta;
4. A nomenclatura utilizada na geração dos identificadores, quer seja para colaboradores internos quer para entidades externas, obedece a regras a definir;
5. Devem ser definidas regras que regulem a nomenclatura a adotar na criação de *user Ids*;
6. O identificador do utilizador permite reconhecer a sua identidade, mas nunca os seus níveis de privilégio;
7. O identificador deve ser pessoal, intransmissível e único para todos os sistemas, se tecnicamente viável;
8. Os identificadores pertencentes a colaboradores do Município de Alvaiázere ou de entidades externas que já saíram ou já não têm um vínculo contratual, não podem ser atribuídos a outros colaboradores internos e de entidades externas;
9. Para as eventuais exceções, fica registado, e em histórico, qual foi a pessoa que esteve associada a um *user ID* e durante que período de tempo.

Artigo 37.º - Acessos privilegiados

1. Os acessos privilegiados obedecem a todas as regras definidas anteriormente e, adicionalmente, devem ter uma autorização especial, no processo de gestão de acessos;

2. Os acessos privilegiados, quando necessários, são atribuídos a um identificador (*user ID*) especial, diferente do identificador usual do utilizador;
3. Os acessos privilegiados têm um período de validade de 3 meses, ao fim do qual o utilizador terá de confirmar a sua necessidade de continuar com o acesso, caso contrário este é revogado;
4. Os acessos atribuídos no âmbito de operações de emergência têm um período de validade de 8 dias;
5. Sempre que possível, são criadas rotinas de sistema ou programas automatizados de forma a minimizar a necessidade de atribuição de acessos privilegiados aos utilizadores.

Artigo 38.º - Entidades externas

1. Os acessos atribuídos a entidades externas aos sistemas do Município de Alvaiázere obedecem às regras e princípios definidos nesta secção;
2. Têm um período de validade associado à duração do seu contrato com o Município de Alvaiázere, ao fim do qual o responsável pelo contrato terá de justificar a sua necessidade de continuar com o acesso;
3. Caso o responsável pelo contrato não consiga justificar a necessidade de continuar com o acesso, este é revogado.

Artigo 39.º - Revisão dos privilégios de acesso

1. Os privilégios de acesso dos utilizadores são revistos, pelo menos, uma vez por ano, pelo serviço de TI em coordenação com a hierarquia do respetivo utilizador, de forma a garantir que os acessos aprovados continuam a ser válidos;
2. Os privilégios de acesso dos utilizadores são revistos sempre que ocorra uma alteração, como uma saída, uma mudança de funções ou de área;
3. Os acessos privilegiados são revistos a cada 3 meses;
4. As alterações às contas privilegiadas são guardadas para efeitos de revisão periódica;
5. Os privilégios de acesso implementados nos sistemas são sujeitos a um processo automático de monitorização contínua que permite detetar/corrigir incoerências com os acessos aprovados.
6. Excecionalmente, nos casos em que tecnicamente não é possível um processo automático, esta revisão a que alude o número anterior é feita manualmente.

Artigo 40.º - Condicionantes e exceções

1. A aplicação das normas constantes desta secção deve ser sujeita a um processo de gestão de alterações, as quais poderão dar origem a projetos de manutenção evolutiva;
2. Estas boas práticas irão sendo aplicadas ao longo do tempo, tendo em consideração:
   a) As limitações tecnológicas de cada aplicação;
   b) As características organizacionais do Município de Alvaiázere;
3. Caso algum dos sistemas não permita tecnicamente a aplicação de algum dos princípios, a situação fica identificada numa lista de exceções e são criados os controlos compensatórios adequados.

SECÇÃO II - Processo de Gestão de Acessos

Artigo 41.º - Gestão de acessos

1. As contas dos utilizadores do domínio cm-alvaiazere.pt são criadas no sistema pelos elementos do serviço de TI:
   a) por solicitação dos responsáveis, quando se trate de entidades externas à entidade;
   b) por iniciativa do serviço de TI, quando se trate de contas internas dos sistemas ou de outros utilizadores não previstos nos números anteriores;
2. Os pedidos de criação de contas previstas na alínea a) do número anterior são efetuados por email a um elemento do serviço de TI;
3. A criação das contas previstas na alínea b) do número 1 deverá ficar fundamentada em documento onde se registe o objetivo das mesmas;
4. Numa segunda fase, e se necessário, o Chefe de Divisão ou responsável do colaborador, comunica ao serviço de TI outras permissões e acessos a atribuir nas aplicações ou informação de que é responsável;
5. Os pedidos enviados ao serviço de TI devem conter todas as informações necessárias, designadamente as permissões de acesso às aplicações e/ou pastas partilhadas, em conformidade com as atividades realizadas pelos utilizadores, bem como a concessão, ou não, de acesso à internet;
6. Para efeitos do número anterior, no caso das contas dos colaborares da entidade, será o Chefe de Divisão ou responsável do colaborador a comunicar ao serviço de TI estas informações;
7. A todos os colaboradores do Município de Alvaiázere é atribuída uma conta de email profissional;
8. A nova conta de utilizador só pode ser aberta quando o serviço de TI dispuser de todas as informações que julgar necessárias. Para o efeito, o serviço de TI deve solicitar as informações em falta.

Artigo 42.º - Alteração de permissões e acessos de contas de utilizadores

1. A alteração de permissões de acesso atribuídas a uma determinada conta só pode ser solicitada ao serviço de TI pelo responsável da secção desse utilizador;
2. O pedido a que alude o número anterior deve ser formalizado em email enviado a um elemento do serviço de TI.

Artigo 43.º - Desativação e anulação de contas de utilizadores

1. A conta deve ser bloqueada após 5 tentativas de acesso mal sucedidas, devendo o utilizador solicitar ao serviço de TI a reativação da sua conta;
2. Para efeitos do número anterior, designa-se por bloqueio a desativação da conta por erro de *login* do utilizador;
3. Uma conta pode ser desativada a pedido da entidade que determinou a sua criação, do responsável da Divisão ou pela sua hierarquia superior;
4. A título excecional e devidamente fundamentado, ao serviço de TI pode desativar temporariamente uma conta;
5. O pedido de anulação definitivo das contas é efetuado pela entidade que determinou a sua criação, pelo responsável do serviço ou pela sua hierarquia superior, sendo que neste caso, a conta é num primeiro momento, desativada;
6. Uma conta só pode ser eliminada após ter estado desativada, pelo menos, 6 meses;
7. Para efeitos no número anterior, é efetuado anualmente um controlo das contas desativadas;
8. Semestralmente, o serviço de TI verifica se as contas ativas devem estar neste estado.

SECÇÃO III - Política de gestão de *passwords*

Artigo 44.º - Atribuição de *passwords*

1. Os utilizadores assinam um termo de responsabilidade em como se comprometem a manter as *passwords* individuais confidenciais e em como não revelam as *passwords* de grupo, associadas às contas genéricas, para fora dos membros do grupo;
2. É estabelecido um procedimento de validação da identidade do utilizador antes de lhe ser atribuída uma *password* de substituição temporária.

Artigo 45.º - Regras de composição de *passwords*

1. As *passwords* utilizadas nos sistemas do Município de Alvaiázere são individuais, apenas do conhecimento do próprio utilizador e obedecem a regras de composição, que são verificadas automaticamente sempre que os utilizadores alteram/definem a sua *password*;
2. As regras de composição das *passwords* estão descritas em documento próprio, incluído nas políticas de segurança (Anexo I);
3. A *password* dos utilizadores é criada pelo serviço de TI e entregue diretamente ao colaborador em envelope fechado, onde estão também descritas as regras de composição das *passwords*.
4. Após primeiro login, será posteriormente e de forma automática, solicitada a alteração da password temporária que lhe foi fornecida.

Artigo 46.º - Gestão de *passwords*

1. As novas *passwords* atribuídas aos utilizadores e as *passwords* de substituição temporárias devem ser únicas para um utilizador, devendo obedecer às regras definidas nesta secção, de forma a não serem simples de prever;
2. As *passwords* são fornecidas aos utilizadores por um canal seguro.
3. A utilização de serviços de correio eletrónico público ou em "*clear-text*" deve ser evitada;
4. Os utilizadores confirmam a receção das *passwords*;
5. As *passwords* atribuídas aos utilizadores expiram automaticamente no momento da primeira tentativa de autenticação com sucesso, obrigando à respetiva alteração imediata;
6. As *passwords* por omissão dos sistemas são alteradas após a instalação dos mesmos;
7. As *passwords* atribuídas aos utilizadores no âmbito de um dado sistema expiram automaticamente a cada 120 dias, obrigando à respetiva alteração;
8. Sempre que permitido tecnicamente pelo sistema, as *passwords* não podem ser reutilizadas por um mesmo utilizador antes de 5 iterações;
9. A visualização das *passwords* é mascarada, suprimida, ou, de alguma forma, protegida da observação de terceiros;
10. As *passwords* não devem ser guardadas nos sistemas de forma desprotegida;
11. Não são permitidas *passwords* embebidas no código das aplicações e sistemas, salvo se formalmente aprovado pelo serviço responsável pelo desenvolvimento em causa e pelo representante do serviço de TI;
12. Caso algum dos sistemas do Município de Alvaiázere não permita tecnicamente a aplicação de algum dos princípios anteriores, esta situação fica identificada numa lista de exceções e são criados os mecanismos alternativos adequados.

Artigo 47.º - Responsabilidade dos utilizadores

1. Os utilizadores devem manter as *passwords* confidenciais, não as revelando de nenhuma forma;
2. Os utilizadores não devem registar as *passwords*, seja em papel ou em formato digital, exceto se o método tiver sido aprovado na organização e permita que as *passwords* sejam guardadas de uma forma segura;
3. Os utilizadores devem alterar a *password* sempre que exista informação de um possível comprometimento da *password* ou do sistema;
4. Os utilizadores devem escolher *passwords* fortes e que cumpram as regras definidas pela organização para a complexidade das mesmas;
5. Os utilizadores devem alterar as *passwords* em intervalos regulares, mesmo quando não é exigido pelo sistema, e evitar reutilizar *passwords* previamente usadas;
6. As *passwords* de contas privilegiadas devem ser alteradas mais frequentemente;
7. Os utilizadores devem alterar as *passwords* que lhes são atribuídas temporariamente no primeiro *logon*;
8. Os utilizadores não devem incluir as *passwords* em nenhum processo automático;
9. Os utilizadores não devem partilhar as suas *passwords* individuais;
10. Os utilizadores não devem partilhar as *passwords* de contas de grupo para fora dos elementos pertencentes ao grupo;
11. Os utilizadores não devem utilizar as mesmas *passwords* para uso pessoal e profissional.

Artigo 48.º - Autenticação forte

Para acessos VPN, acessos a sistemas mais críticos ou para mecanismos de autenticação partilhadas por vários sistemas, devem ser implementados, sempre que possível, mecanismos de autenticação forte (exemplo: OTP, *passwords* + certificados digitais, *tokens*, impressão digital, etc.).

Artigo 49.º - Condicionantes e exceções

1. As boas práticas enunciadas nesta secção são implementadas logo que possível, tendo em consideração:
   a) as limitações tecnológicas de cada aplicação;
   b) as características organizacionais do Município de Alvaiázere;
2. Caso algum dos sistemas não permita tecnicamente a aplicação de alguma destas regras, deve esta situação ficar identificada numa lista de exceções e, sempre que possível, devem ser criados os controlos compensatórios adequados.

SECÇÃO IV - *Logging* e Monitorização

Artigo 50.º - Monitorização da utilização de sistemas

1. O uso das infraestruturas de processamento de informação é monitorizado e os resultados das atividades de monitorização são revistos regularmente;
2. As atividades de monitorização das infraestruturas devem cumprir com os requisitos legais relevantes e regulamentações;
3. É monitorizado o acesso autorizado às infraestruturas de processamento de informação, acompanhando os *user IDs*, a data e hora dos eventos chave como *login* e *logoff*, os tipos de evento, os ficheiros acedidos, as aplicações, bases de dados utilizadas e todas as operações privilegiadas;

4. São monitorizadas as operações e atividades privilegiadas, acompanhando a utilização de todas as contas privilegiadas, como a utilização de todas as contas de administração, supervisão e *root*, os arranques e paragens de todos os sistemas, os serviços, todas as ligações e desconexões de dispositivos de entrada/saída;
5. São monitorizadas todas as tentativas não autorizadas de acesso às infraestruturas de processamento de informação, acompanhando todas as ações dos utilizadores rejeitadas ou falhadas, incluindo as que envolvam dados, as notificações de *firewalls*, sistemas operativos, domínio e equipamentos de segurança;
6. São monitorizados os alertas dos sistemas de informação, as falhas nos sistemas, alertas e mensagens de consola, alarmes de gestão de rede, alarmes de controlos de acesso e exceções de *logs* de sistema;
7. São monitorizadas as alterações e tentativas de alteração aos controlos de segurança dos sistemas;
8. Os resultados da monitorização devem ser revistos regularmente e consoante a criticidade do sistema;
9. As áreas de elevado risco são revistas com maior frequência que as de menor risco;
10. Os resultados da monitorização de aplicações e sistemas críticos são revistos com maior frequência que os de não críticos;
11. Os resultados da monitorização de informação crítica ou sensível são revistos com maior frequência;
12. Os resultados da monitorização de sistemas onde já ocorreram falhas de segurança, com maior grau de vulnerabilidade ou que tiveram o sistema de *log* desativado, são revistos com maior frequência que os sistemas onde estas situações não se verificam;
13. Os resultados da monitorização de sistemas ligados em rede são revistos com maior frequência que os sistemas isolados.

Artigo 51.º - *Logs* de auditorias

1. O nível de *logs* é definido, durante a análise de risco para cada um dos sistemas, de acordo com a criticidade e a capacidade técnica do respetivo sistema;
2. São gerados *logs* de sistema para registar os *user IDs*, as datas e horas, os detalhes dos eventos chave, as entradas e saídas nos sistemas, a identificação dos terminais e, se possível, a sua localização, tentativas de acesso aos sistemas bem sucedidas e rejeitadas;
3. São gerados *logs* de sistema para registar alterações à configuração dos sistemas, a utilização de privilégios, o recurso a utilitários de sistema, os ficheiros acedidos e como são acedidos, os endereços de rede, os protocolos e os acessos aos alarmes de controlo de sistema;
4. São gerados *logs* de sistema para registar a ativação e desativação de proteções de sistema, como antivírus e sistemas de deteção de intrusão.

Artigo 52.º - *Logs* de operação e administração

1. As atividades dos administradores e operadores de sistema são registadas em *logs*;
2. Os *logs* de operação e administração de sistemas são revistos regularmente;
3. Deve-se garantir que fica guardada em *log* a informação sobre eventos e falhas de sistema, quais os processos envolvidos, que eventos ocorreram com e sem sucesso, ocorrências associadas à manipulação de ficheiros, erros de sistema e a conta envolvida.

Artigo 53.º - *Logs* de falhas

1. As falhas são registadas em *logs*, analisadas e tomadas as devidas ações;

2. A informação sobre falhas e erros de processamento ou comunicações reportadas por utilizadores ou por programas de sistema é registada em *log*;
3. Deve ser garantido que o registo de erros está ativo, sempre que os sistemas suportem esta funcionalidade;
4. As regras sobre como tratar as falhas ou erros reportados devem ser definidas;
5. Os *logs* de falhas são revistos de forma a garantir que os erros e falhas reportadas foram resolvidos e/ou que as medidas corretivas foram tomadas;
6. As medidas a tomar para correção de falhas ou erros detetados seguem um processo formal de gestão de alterações, de forma a garantir que são corretamente autorizadas e que os controlos de segurança não são comprometidos.

Artigo 54.º - Proteção de *Logs*

1. As infraestruturas que geram *logs* e a informação desses *logs* são protegidos contra alterações e acessos não autorizados; Os logs devem ser encriptados no ato de coleta, transmitidos de forma segura e armazenados de forma forense com certificados digitais, de forma a garantir que não houve qualquer alteração ao seu conteúdo.
2. São definidos controlos para proteção contra alterações não autorizadas às infraestruturas que produzem *logs* e às informações de *log*, de forma a evitar:
   a) problemas operacionais com as infraestruturas de *log*;
   b) alteração ao tipo de mensagem registada;
   c) alteração ou mesmo remoção dos ficheiros de *log*;
   d) que os ficheiros de *log* gerem problemas de capacidade.
3. Os *logs* são armazenados de forma a cumprir a norma de retenção de registos do Município de Alvaiázere e com os requisitos da recolha e retenção de evidências.

Artigo 55.º - Sincronização de relógio

1. Os relógios de todos os sistemas de processamento de informação relevantes são sincronizados com uma fonte considerada exata;
2. É definido um procedimento de verificação dos relógios dos sistemas e corrigem-se variações significativas nas horas;
3. Deve ser garantido que os formatos de data e hora são corretamente interpretados;
4. Deve ainda ser garantida a correta interpretação dos *timestamps* que incorporam as condições locais.

SECÇÃO V - Gestão de Incidentes

Artigo 56.º - Âmbito

As normas constantes da presente secção aplicam-se às atividades a desenvolver no âmbito do processo de gestão de incidentes (*Incident Management*) e a gestão de incidentes de segurança, segundo a norma ISO27001.

Artigo 57.º - Reportar eventos de segurança de informação

1. São implementados e mantidos os procedimentos formais de reporte, escalamento e resolução de eventos;

2. Todos os utilizadores do sistema informático devem estar conscientes dos procedimentos para reportar os diferentes tipos de eventos e de vulnerabilidades que possam ter impacto na segurança de informação dos ativos do Município de Alvaiázere.
3. O reporte do incidente de segurança pode ser realizado telefonicamente, por email ou plataforma de gestão de serviço de TI que venha a ser divulgada para o efeito;
4. O procedimento para reportar eventos de segurança de informação deve indicar um ponto de contacto, o qual deve ser do conhecimento geral de todo o Município de Alvaiázere;
5. O ponto de contacto está sempre disponível e, quando solicitado, deve responder adequada e atempadamente;
6. Todos os utilizadores do sistema informático devem conhecer o procedimento para reportar eventos de segurança de informação e devem ser informados da necessidade de os reportar prontamente, pelo que para o efeito será enviado um email (Anexo II);
7. O procedimento para reportar os eventos pode incluir um formulário, em papel ou formato eletrónico, para reportar e registar os eventos de segurança de informação, onde devem ser incluídos todos os detalhes pertinentes associados ao evento, nomeadamente o tipo de falha, eventuais mensagens nos ecrãs e, adicionalmente, quaisquer outros aspetos estranhos;
8. O procedimento para reportar eventos de segurança de informação deve incluir atividades de *feedback* para assegurar que as pessoas são informadas dos resultados alcançados;
9. O procedimento para reportar eventos de segurança de informação deve esclarecer que serão alvo de processos disciplinares todos aqueles que permitirem fugas de informação que comprometam a segurança de informação.

Artigo 58.º - Reportar vulnerabilidades de segurança de informação

1. Os incidentes de segurança de informação devem ser prevenidos, assegurando-se de que todos os utilizadores estão conscientes da necessidade de reportar prontamente vulnerabilidades observadas ou suspeitas de segurança de informação, seguindo o procedimento para reportar as vulnerabilidades definido para reportar incidentes de segurança de informação;
2. Deve-se garantir que todos os colaboradores compreendem que não devem tentar testar uma vulnerabilidade suspeita ou provar que é real, mas sim reportá-la rapidamente.

Artigo 59.º - Responsabilidades e procedimentos

1. É estabelecido um procedimento formal de gestão de incidentes de segurança de informação que identifica responsabilidades e que permite assegurar uma resposta rápida, efetiva e ordenada, identificando as ações a desenvolver sempre que é reportado um incidente de segurança de informação;
2. Os procedimentos para reportar e gerir incidentes e vulnerabilidades de segurança de informação devem responder a uma grande variedade de tipos de incidentes;
3. O procedimento de gestão de incidentes deve obrigar à identificação e análise de causas dos incidentes de segurança de informação, ao planeamento e a implementação de ações corretivas e preventivas e, quando aplicável, à implementação de medidas de contenção dos efeitos dos incidentes;
4. As ações corretivas e preventivas são reportadas a quem detenha autoridade apropriada sobre a natureza e resultados das ações;
5. O procedimento de gestão de incidentes deve assegurar que os responsáveis pelo tratamento comunicam com os afetados pelo incidente a sua resolução ou atrasos na resolução;
6. O procedimento de gestão de incidentes deve assegurar que, sempre que necessário, sejam analisados os registos de auditorias e que sejam obtidas as evidências dos incidentes e problemas de segurança de informação;
7. As evidências obtidas são utilizadas para análise de contratos, verificar violações a regulamentos, suportar procedimentos legais, analisar a má utilização de computadores, confrontar com a

legislação de proteção de dados e negociar compensações com os fornecedores de *software* e prestadores de serviços;

8. O procedimento de recuperação deve assegurar que somente pessoas autorizadas poderão aceder a sistemas e dados reais do Município de Alvaiázere, que todas as ações desenvolvidas são documentadas detalhadamente, que as ações e os seus resultados são comunicados à CSI e que esta revê atentamente aquela informação;
9. Os incidentes de segurança de informação são usados, com as devidas reservas de confidencialidade, na formação e consciencialização do pessoal como exemplos do que pode acontecer, como responder a tais incidentes e de como evitá-los no futuro;
10. Devem existir mecanismos que permitam a quantificação e a monitorização dos tipos, volumes e custos dos incidentes de segurança de informação;
11. Os incidentes de segurança de informação devem ser avaliados para identificar a sua recorrência e para identificar aqueles que tenham impacto elevado para o Município de Alvaiázere;
12. A CSI deve usar a experiência e aprendizagem adquiridas sobre os incidentes de informação no Município de Alvaiázere para melhorar os controlos, para reduzir a frequência, os danos e os custos potenciais de futuros incidentes de segurança de informação e, se necessário, rever a Política e Normas de Segurança de Informação.

Artigo 60.º - Gestor do processo de gestão de acidentes

A CSI, enquanto gestora do processo de gestão de incidentes, é responsável por:

a) desenhar e responder pelo processo e definir as respetivas métricas e gerir as alterações necessárias ao processo e às métricas;
b) definir a política para o processo e *standards* a usar na sua execução;
c) rever regularmente a estratégia para o processo para assegurar que se mantém adequada e promover a sua alteração quando necessária;
d) colaborar com os responsáveis por outros processos para assegurar que existe uma aproximação integrada para a definição e implementação da gestão de incidentes, problemas, eventos, acessos e pedidos;
e) assegurar que o processo tem documentação apropriada e que esta está atualizada e disponível;
f) auditar regularmente o processo para assegurar a conformidade com a política e *standards* definidos.

Artigo 61.º - Recolha de evidências

1. Sempre que, após um incidente de segurança de informação, uma ação de seguimento sobre pessoas ou organizações implique uma ação legal, seja esta civil ou criminal, as evidências são recolhidas, guardadas e apresentadas em conformidade com as regras de provas e evidências, sempre em concordância com a normatividade jurídica vigente;
2. Deve ser assegurado que as evidências recolhidas são admissíveis e que podem ser formalmente usadas em tribunal;
3. Deve ser protegida a qualidade e a integridade das evidências para assegurar que estas suportam a posição legal do Município de Alvaiázere;
4. Deve ser assegurada a capacidade de prova de que os controlos do processo estão a trabalhar correta e consistentemente e que podem, consequentemente, proteger a qualidade das evidências processadas e armazenadas nos sistemas de informação;
5. Deve ser assegurado que a qualidade das evidências é suficiente para suportar quaisquer ações legais;
6. Deve ser assegurado que os originais das evidências não são alterados e devem ser feitas cópias das evidências e guardadas fora do perímetro do Município de Alvaiázere;

7. Devem ser mantidos os ficheiros de registo (*log*) de todas as ações de cópia de evidências para efeitos disciplinares e o processo de cópia deve ser testemunhado;
8. Deve ser assegurado que a informação relacionada com incidentes de segurança de informação não é destruída acidental ou intencionalmente durante as investigações aos incidentes;
9. Devem ser informados os órgãos com competência na matéria, o mais cedo possível, sempre que se preveja que dum incidente sério de segurança de informação possa resultar uma ação legal.

SECÇÃO VI - Política de Conformidade

Artigo 62.º - Identificação da legislação aplicável

1. O desenho, operação, utilização e administração de sistemas de informação devem obedecer aos requisitos legais, regulatórios e contratuais;
2. Sempre que se justifique deve-se procurar aconselhamento jurídico sobre exigências legais específicas;
3. Todos os requisitos legais, regulatórios e contratuais relevantes e a abordagem do Município de Alvaiázere para cumprir estes requisitos devem ser definidos explicitamente, documentados e mantidos atualizados para cada sistema de informação e para o Município de Alvaiázere;
4. Devem ser identificados e documentados os controlos que necessitam de estar conformes com os requisitos legais, regulatórios e contratuais.

Artigo 63.º - Direitos de propriedade intelectual

1. Devem ser implementados os procedimentos apropriados para assegurar a conformidade com os requisitos legais, regulatórios e contratuais no uso do material para o qual possam existir direitos de propriedade intelectual e no uso de produtos de *software* proprietário;
2. Devem ser criados procedimentos que obriguem à compra de produtos de *software* apenas a fornecedores idóneos;
3. Deve ser mantido um registo de *software* e da informação propriedade do Município de Alvaiázere;
4. Devem ser criados procedimentos para permitir ao Município de Alvaiázere provar que possui todas as licenças de *software*, o original do *software*, manuais e outros recursos de informação que estão a ser utilizados;
5. Deve existir um controlo da manutenção de licenças de *software* e das condições de licenciamento;
6. Devem ser criados controlos que permitam assegurar que não se excede o número máximo de utilizadores permitido para cada produto de *software* proprietário;
7. Deve existir um controlo que assegure que apenas estão a ser utilizados os produtos de *software* legalmente autorizados.

Artigo 64.º - Proteção dos registos do Município de Alvaiázere

1. Os registos importantes devem ser protegidos contra perdas, destruição ou falsificação, de acordo com os requisitos legais, regulatórios, contratuais e de serviço;
2. Os registos são identificados e classificados, de acordo com os níveis de classificação definidos, para que sejam geridos de forma adequada;
3. Deve ser garantido que todas as infraestruturas de armazenamento são tratadas conforme as especificações e recomendações dos fabricantes;
4. Os registos são protegidos contra a possível deterioração das infraestruturas de armazenamento;
5. Deve ser garantido que os registos eletrónicos se encontram acessíveis ao longo do período de retenção, mesmo que as tecnologias tenham mudado;

6. Devem ser selecionados sistemas de armazenamento de dados que permitam recuperar a informação num formato aceitável e dentro de um prazo razoável definido pelo Município de Alvaiázere;
7. A definição dos períodos de retenção de registos é estabelecida de acordo com a legislação e regulamentação aplicável;
8. Devem ser criados controlos para proteger os registos e a informação, a sua perda, destruição ou falsificação.

Artigo 65.º - Proteção de dados e privacidade da informação pessoal

1. A proteção de dados e a privacidade devem ser asseguradas como requerido na legislação e regulamentação relevantes e, se aplicável, nas cláusulas contratuais;
2. Deve ser estabelecida uma proteção corporativa de dados e uma política de privacidade, que deve ser comunicada a todos os envolvidos no processamento de informação pessoal;
3. Deve ser garantido que os princípios de proteção de dados pessoais e os esforços de consciencialização estão de acordo com a regulamentação e legislação em vigor;
4. A CSI deve auxiliar os utilizadores e fornecedores de serviços a proteger a privacidade da informação e indicar-lhes quais as suas responsabilidades e quais os procedimentos que devem seguir;
5. Devem ser desenvolvidas e implementadas medidas organizacionais e técnicas apropriadas para proteger a informação pessoal.

Artigo 66.º - Regulamentação dos controlos criptográficos

1. Os controlos criptográficos são utilizados de acordo com os acordos relevantes, leis e regulamentação;
2. Antes de se decidir sobre a importação ou exportação de *software* ou *hardware* para executar funções criptográficas, devem ser consideradas as suas restrições legais ou outras restrições;
3. Antes de utilizar tecnologias de encriptação, devem ser analisadas as suas restrições;
4. Deve ser obtido aconselhamento legal para assegurar que o acesso ou utilização de controlos criptográficos está em conformidade com a regulamentação, legislação e acordos contratuais.

Artigo 67.º - Prevenção da utilização indevida das infraestruturas de processamento de informação

1. Os utilizadores estão impedidos de utilizar as infraestruturas de processamento de informação para fins não autorizados;
2. Toda a utilização das infraestruturas de processamento de informação deve ser autorizada previamente pela CSI e qualquer utilização das mesmas sem autorização é inaceitável;
3. Deve ser indicada a necessidade de monitorizar a utilização das infraestruturas de processamento de informação para detetar atividades não autorizadas;
4. A utilização sem autorização das infraestruturas de processamento de informação é comunicada à CSI do Município de Alvaiázere;
5. Deve ser assegurado que os colaboradores e entidades externas entendem que têm que receber autorização antes que lhes seja permitido o acesso às infraestruturas de processamento de informação do Município de Alvaiázere.

Artigo 68.º - Conformidade com políticas e normas de segurança de informação

1. A segurança de informação dos sistemas de informação é revista regularmente;
2. As revisões são executadas de acordo com as normas de segurança de informação. As plataformas técnicas e os sistemas de informação devem ser auditadas para verificar a conformidade com os controlos de segurança de informação documentados;
3. A CSI assegura que todos os procedimentos de segurança de informação na sua área de responsabilidade são executados corretamente para atingir a conformidade com as políticas e normas de segurança de informação;
4. Deve ser garantido que a CSI entende as causas das não conformidades antes de efetuar ações de remediação;
5. A CSI deve implementar ações preventivas e corretivas e avaliar essas ações para verificar a sua efetividade;
6. Devem existir controlos que garantam que são registadas as ações preventivas e corretivas efetuadas para tratar problemas de não conformidade associados à segurança de informação. Estes registos devem ser mantidos e atualizados de forma contínua;
7. Deve ser garantido o registo das revisões de segurança de informação efetuadas pela CSI com o objetivo de avaliar e verificar a efetividade das ações preventivas e corretivas e que estes registos são mantidos.

Artigo 69.º - Controlo de auditoria dos sistemas de informação

1. É exigida proteção para salvaguardar a integridade e prevenir a má utilização das ferramentas de auditoria;
2. Os requisitos e atividades de auditoria que verifiquem os sistemas operacionais devem ser planeados cuidadosamente e acordados para minimizar os riscos na interrupção de processos de serviço;
3. Deve ser garantido que os requisitos das auditorias são aprovados pela CSI antes da sua execução;
4. Devem ser identificados os recursos necessários para executar testes de auditoria antes do seu início e estar disponíveis na altura de efetuar a auditoria;
5. Deve ser garantido que qualquer requisito de processamento adicional ou especial é identificado e aprovado antes de efetuar a auditoria;
6. Deve ser garantida a identificação da necessidade de guardar a data/hora, no registo de auditoria, para dados ou sistemas críticos;
7. Deve ser indicada a necessidade de documentar todas as exigências, responsabilidades e procedimentos de auditoria aos sistemas de informação;
8. Os auditores têm de ser independentes das atividades e sistemas a auditar.

Artigo 70.º - Verificação da conformidade técnica

1. Os sistemas de informação devem ser verificados regularmente para aferir a conformidade com as normas de segurança de informação;
2. Devem existir controlos que garantam a execução de verificações da conformidade técnica, sempre que possível de forma automática. Caso tal não seja possível, devem ser executadas verificações manuais por especialistas;
3. Os relatórios de conformidade técnica do Município de Alvaiázere devem ser validados por especialistas;
4. Devem existir controlos implementados que assegurem a necessidade de planear, efetuar e documentar testes de intrusão e avaliação de vulnerabilidades de segurança de informação dos sistemas;

5. Os testes de intrusão e avaliação de vulnerabilidades de segurança de informação devem ser repetíveis, feitos de forma a não afetar a segurança de informação dos sistemas e efetuados e supervisionados por técnicos competentes e autorizados.

SECÇÃO VII - Política de segurança para fornecedores

Artigo 71.º - Âmbito

1. As normas vertidas na presente secção estabelecem os princípios e as melhores práticas de segurança a aplicar na relação de fornecedores com o Município de Alvaiázere;
2. A política e os princípios aqui definidos são aplicáveis aos fornecedores do Município de Alvaiázere que forneçam bens e serviços considerados no âmbito do SGSI.

Artigo 72.º - Segurança de fornecedores durante a contratação

1. Todos os candidatos a concurso e entidades externas devem ser adequadamente selecionados, especialmente para funções sensíveis;
2. Os contratos a celebrar com fornecedores devem incluir uma cláusula de confidencialidade, mediante a qual os mesmos se obrigam a manter sob estrita confidencialidade as condições do acordo, bem como quaisquer outras informações que, na execução dele, obtenham acerca do Município e da sua atividade, incluindo ainda toda a informação de natureza organizativa, técnica ou financeira;
3. As entidades externas que sejam utilizadores de infraestruturas de processamento de informação devem assinar um acordo que defina as suas funções e responsabilidades relativamente à segurança de informação, sempre que esta definição não conste dos contratos e acordos celebrados;
4. As funções e as responsabilidades de segurança de informação dos colaboradores e das entidades externas devem ser definidas e documentadas de acordo com a política de segurança de informação do Município de Alvaiázere.

Artigo 73.º - Fornecimento de Serviços

1. O Município de Alvaiázere deve conferir a implementação dos contratos, monitorizar a concordância com os mesmos e gerir as alterações, para assegurar que os serviços entregues estão em concordância com os requisitos acordados com terceiras partes;
2. Deve-se assegurar que os controlos de segurança de informação, as definições do serviço e os níveis de entrega incluídos no acordo do fornecimento de serviços por terceiros são implementados, operacionalizados e mantidos pelos terceiros;
3. Os terceiros devem poder continuar a fornecer serviços após desastres significativos ou falhas de serviço;
4. Os terceiros devem dispor de planos de continuidade de serviço executáveis;
5. Os planos de continuidade de serviço que os terceiros dispõem devem explicar como podem ser mantidos os níveis de serviço acordados, caso ocorra um desastre ou falha de serviço;
6. O Município de Alvaiázere entende que a responsabilidade última é sua, embora as suas atividades de processamento de informação tenham sido passadas por terceiros.

Artigo 75.º - Revisão e monitorização dos serviços de terceiros

1. Os serviços, relatórios e registos fornecidos por terceiros devem ser monitorizados e revistos regularmente e devem ser alvo de auditorias regulares;
2. Os terceiros devem obedecer às condições de segurança de informação e às condições especificadas nos contratos;
3. Deve ser definido um processo para gerir e monitorizar as relações com os terceiros, assim como monitorizar o desempenho dos níveis de serviço destes;
4. Deve ser monitorizado o alinhamento do serviço de terceiros com o acordado;
5. Os registos de auditoria aos terceiros devem ser revistos e esses registos devem ser utilizados para rever eventos de segurança de informação, falhas e problemas operacionais.
6. São utilizados os registos de auditoria das terceiras partes para rastrear falhas no fornecimento do serviço e interrupções no mesmo;
7. Os terceiros devem ter o conhecimento técnico e os recursos necessários para monitorizar e promover o alinhamento com o acordado, assim como para cumprir com os requisitos de segurança de informação.

Artigo 76.º - Gerir alterações nos serviços de terceiros

1. As alterações ao fornecimento dos serviços, incluindo manter e melhorar as normas de segurança de informação, os procedimentos e os controlos existentes devem ser geridas tendo em atenção a criticidade dos sistemas e dos processos do serviço envolvidos e baseadas na reavaliação dos riscos;
2. O Município de Alvaiázere controla como:
   a) são desenvolvidas e implementadas as alterações dos serviços prestados pelos fornecedores;
   b) os fornecedores de serviço terceiros implementam os novos controlos que são desenhados para detetar e comunicar incidentes de segurança de informação ou para melhorar a segurança de informação;
   c) os fornecedores de serviço implementam novas tecnologias, novos produtos ou novas versões (*releases*) dos produtos.

SECÇÃO VIII - Política de secretária limpa e ecrã limpo

Artigo 77.º - Secretária limpa

1. Quando os colaboradores se encontrem a trabalhar na sua secretária, devem garantir que apenas estão expostos os documentos do município que necessitam para as tarefas do seu dia de trabalho, guardando todos os restantes;
2. Sempre que os colaboradores abandonem a sua secretária temporariamente, deverão acautelar que documentos ou dispositivos de armazenamento de informação se encontram guardados num local adequado;
3. Sempre que os colaboradores abandonam a sua secretária por longos períodos de tempo, devem certificar-se que não existem documentos ou dispositivos de armazenamento de informação deixados em cima da secretária.
4. Todos os documentos e dispositivos de armazenamento de informação devem ser guardados num local fechado onde pessoas não autorizadas não possam ter acesso;
5. Devem existir mecanismos alternativos que permitam o acesso de emergência a documentos e dispositivos de armazenamento de informação aos colaboradores autorizados para o efeito;
6. Deve fazer parte das tarefas diárias dos colaboradores a organização e arquivo em segurança dos respetivos documentos ou dispositivos de armazenamento;
7. Os documentos e dispositivos de armazenamento cuja conservação não é necessária devem ser destruídos, obedecendo-se aos procedimentos estabelecidos pelo Município de Alvaiázere para o

efeito e de acordo com a respetiva sensibilidade da informação. Considera-se que deixam de ser necessários os documentos e dispositivos de armazenamento que o responsável hierárquico, tendo em conta a legislação aplicável, assim o entenda;
8. Os dispositivos de identificação físicos dos utilizadores nunca devem ser deixados sem controlo do próprio.

Artigo 78.º - Ecrã limpo

1. Sempre que tecnicamente possível, todos os computadores e servidores devem ter os mecanismos automáticos de autobloqueio ativados e com proteção por *password*;
2. Sempre que os utilizadores abandonam os seus computadores temporariamente devem bloquear o ecrã com proteção por *password*;
3. Sempre que os utilizadores abandonam os seus computadores por longos períodos de tempo devem fechar todas as aplicações e efetuar o *shutdown* da sua estação de trabalho;
4. Em caso de emergência e se for necessário abandonar o local de trabalho os utilizadores devem, se isso for possível, bloquear o ecrã com proteção por *password*, para evitar o acesso ao mesmo de pessoas não autorizadas;
5. Sempre que os utilizadores se encontrem a trabalhar no seu computador devem colocá-lo numa posição que não permita a visualização da informação por parte de pessoas sem necessidade de acesso à mesma.

Artigo 79.º - Exceções

As exceções a qualquer norma plasmada nesta secção, ou aos seus procedimentos, quando permitidas, devem ser aprovadas por escrito pelos responsáveis pelo colaborador, ou por outra pessoa credenciada para o efeito.

Artigo 80.º - Responsabilização dos colaboradores

1. Os colaboradores a quem está afeto um posto de trabalho são responsáveis pela sua correta utilização de acordo com as instruções em vigor no Município de Alvaiázere e dispostas nesta secção;
2. Os colaboradores que detetem uma violação a qualquer uma das regras enunciadas anteriormente deverão comunicá-la de imediato ao seu superior hierárquico ou ao serviço de TI;
3. A utilização incorreta do acesso ao Município de Alvaiázere poderá dar lugar ao cancelamento do mesmo, sem prejuízo das consequências disciplinares que daí possam resultar.

SECÇÃO IX - Utilização de correio electrónico

Artigo 81.º - Utilização de correio eletrónico

1. O sistema de correio eletrónico disponibilizado pelo Município de Alvaiázere destina-se a ser utilizado no desempenho de atividades profissionais;
2. O sistema de correio eletrónico do Município de Alvaiázere deve ser usado de acordo com a legislação e regulamentação vigente, bem como em conformidade com as restantes políticas, normas e procedimentos do Município de Alvaiázere;
3. O Município de Alvaiázere autoriza os seus colaboradores a usarem o sistema de correio eletrónico para fins pessoais, não relacionados com a respetiva função;
4. A utilização prevista no número anterior deverá obedecer ao seguinte:

a) não prejudicar o desempenho profissional e produtividade do colaborador e/ou restantes colaboradores.
b) as mensagens de carácter pessoal destinadas a outros colaboradores do Município de Alvaiázere, não deverão reter a atenção prolongada destes, nomeadamente por motivos de pedido de resposta à mensagem e/ou características da mesma;
c) não é permitido o envio de mensagens não solicitadas de carácter publicitário (SPAM) ou de mensagens em cadeia;
d) os colaboradores devem criar pastas próprias, devidamente identificadas, de arquivo das mensagens eletrónicas de conteúdo pessoal de forma a que não exista mistura de mensagens profissionais e pessoais nas mesmas pastas.

5. Não é permitido utilizar o sistema de correio eletrónico no âmbito de outra atividade profissional, estranha à relação contratual com o Município de Alvaiázere;
6. É proibido o uso do correio eletrónico para enviar ou guardar mensagens que contenham comentários e/ou imagens que evidenciem uma linguagem imprópria ou desrespeito, nomeadamente afirmações de carácter sexual, racial, religioso ou cujo conteúdo seja, de alguma forma, ofensivo, discriminatório, obsceno, assediador, ameaçador ou fraudulento;
7. É fortemente desaconselhado o uso do endereço de correio eletrónico atribuído ao utilizador do Município de Alvaiázere para registo em sites não corporativos como sejam redes sociais, sites de jogos, sites de relacionamentos, sites de comércio eletrónico, sites de notícias e outras que se mostrarem inconvenientes;
8. As mensagens de correio eletrónico não devem ser reencaminhadas automaticamente para outra caixa de correio, exceto se for do município por forma a assegurar a continuidade de serviço;
9. O reencaminhamento para fora da rede do Município de Alvaiázere deve ser evitado;
10. Os utilizadores não podem enviar mensagens de correio eletrónico contendo informação interna, exceto por necessidades profissionais;
11. A inclusão de endereços externos em listas internas de distribuição deve ser evitada, a fim de obstar qualquer transferência acidental de informação interna para o exterior.

Artigo 82.º - Informação sensível

1. Os utilizadores deverão garantir que não transmitem mensagem de correio eletrónico contendo informação classificada como confidencial através de redes públicas consideradas inseguras, como é o caso da Internet, ou no caso de necessitarem de o fazer, devem cifrá-las;
2. As mensagens de correio eletrónico devem incluir assinaturas digitais quando estas forem de caracter legal ou contratualmente exigidas;
3. A inclusão de endereços externos em listas internas de distribuição não é autorizada, a fim de evitar qualquer transferência acidental de informação confidencial ou de uso interno para o exterior;
4. É proibido o envio de informação considerada de natureza sensível, no âmbito do Regulamento Geral de Proteção de Dados (avaliações de colaboradores, dados clínicos, dados biométricos, entre outros) para endereços de email internos ou externos ao Município de Alvaiázere sem devida autorização do superior hierárquico;
5. Os colaboradores do Município de Alvaiázere devem assegurar que o envio das mensagens apenas é feito para quem necessita de as receber, evitando a sua difusão para além do necessário.
6. Não é autorizado utilizar o sistema de correio eletrónico para difundir dados protegidos por direitos de propriedade intelectual e industrial, em violação das leis de proteção e *copyright* aplicáveis.

Artigo 83.º - Segurança das *passwords* de acesso ao correio eletrónico

1. Os identificadores e as *passwords* que garantem a identificação dos utilizadores no sistema de correio eletrónico e a privacidade dos respetivos conteúdos são propriedade do utilizador e não devem ser partilhados com outros utilizadores;
2. A salvaguarda das *passwords* de acesso ao correio eletrónico é da responsabilidade do utilizador aos quais estas foram atribuídas;
3. Os colaboradores são responsáveis por todas as mensagens transmitidas com a sua conta de correio eletrónico;
4. Um utilizador de uma conta de correio eletrónico não deve poder aceder à conta de correio eletrónico de outro utilizador, a não ser que lhe seja permitido acesso pelo utilizador da respetiva conta;
5. O acesso a mail boxes institucionais deve ser restringido e controlado.

Artigo 84.º - *Disclaimer*

Todas as mensagens têm de finalizar com a seguinte comunicação de isenção:

"*O conteúdo desta mensagem eletrónica e de todos os ficheiros em anexo são confidenciais e podem conter informação privilegiada. Quem dela tomar conhecimento sem autorização do emitente poderá incorrer em ilícito penal. Estão estritamente interditas a publicação, distribuição, uso, impressão ou cópia não autorizadas da mensagem ou dos seus anexos. Caso tenha recebido esta mensagem por engano, queira por favor devolver-nos a mensagem errónea. Obrigado pela sua colaboração.*"

Artigo 85.º - Deteção e remoção de código malicioso

1. Todas as mensagens de correio eletrónico serão analisadas automaticamente por um sistema de deteção e remoção de vírus informáticos;
2. As mensagens infetadas com vírus poderão ser automaticamente eliminadas;
3. Devem ser seguidas pelos utilizadores as seguintes regras que complementam as medidas tomadas pelo Serviço de TI:
   a) nunca abrir quaisquer ficheiros ou macros anexos a um email vindo de uma fonte desconhecida, suspeita ou não confiável. Neste caso, o utilizador deverá informar o serviço de TI para que este proceda à análise prévia da mensagem, ou proceder à sua destruição;
   b) nunca fazer *downloads* de ficheiros a partir de fontes desconhecidas ou suspeitas;
   c) apagar mensagens publicitárias não solicitadas (SPAM) e *SCAM* em cadeia sem as reenviar;
   d) ignorar mensagens, conjeturando sobre ameaças de vírus e sua respetiva eliminação, exceto se vindas do serviço de TI.

Artigo 86.º - Limites do correio eletrónico

1. O serviço de correio eletrónico é limitado no tamanho máximo por mensagem para assegurar que os recursos adequados estão disponíveis para todos os utilizadores do sistema;
2. As mensagens de correio eletrónico não devem exceder os seguintes valores:
   a) Numa conta de email geral, os 2Mb;
   b) Em contas de email de técnicos/apoio administrativo, os 2Mb;
   c) Em contas de email de dirigentes, os 10Mb;
   d) Em contas de email de grupo, os 20Mb;
   e) Em contas de email supra (24h) não se aplicam limites;
3. As exceções aos limites do número 2 têm de ser pedidas e aprovadas;

4. O serviço de correio eletrónico tem um limite de armazenamento de mensagens no Servidor por tipo de conta de email e respeita os seguintes valores:
   a) Numa conta de email geral, o limite de armazenamento é de 512Mb, sendo o aviso aos 450Mb e o bloqueio aos 512Mb;
   b) Em contas de email de técnicos/apoio administrativo, o limite de armazenamento é de 640Mb, sendo o aviso aos 512Mb e o bloqueio aos 640Mb;
   c) Em contas de email de dirigentes, o limite de armazenamento é de 700Mb, sendo o aviso aos 600Mb e o bloqueio aos 700Mb;
   d) Em contas de email de grupo, o limite de armazenamento é de 1024Mb, sendo o aviso aos 900Mb e o bloqueio aos 1024Mb;
   e) Em contas de email supra (24h) não se aplicam limites;
5. As contas de correio eletrónico que excedam o limite definido no "aviso" recebem uma mensagem de notificação, ficando proibidas de enviar novas mensagens a partir do limite definido no "bloqueio";
6. As mensagens de correio eletrónico devem respeitar o número máximo de destinatários em simultâneo, definido segundo o tipo de conta de e-mail, de acordo com o seguinte:
   a) Numa conta de email geral, não existe número máximo de destinatários em simultâneo internamente e existe um limite de 5 destinatários em simultâneo externamente;
   b) Em contas de email de técnicos/apoio administrativo, não existe número máximo de destinatários em simultâneo internamente e existe um limite de 10 destinatários em simultâneo externamente;
   c) Em contas de email de dirigentes, não existe número máximo de destinatários em simultâneo internamente nem externamente;
   d) Em contas de email de grupo, não existe número máximo de destinatários em simultâneo internamente nem externamente;
   e) Em contas de email supra (24h) não se aplicam limites.

Artigo 87.º - Administração

1. O serviço de TI responsável pelo serviço de correio eletrónico pode aceder ao correio eletrónico durante as sessões normais para administração do sistema ou para resolução de problemas;
2. O serviço de TI responsável pelo serviço de correio eletrónico reserva-se o direito de auditar qualquer correio eletrónico para verificar a sua conformidade com as políticas definidas;
3. O serviço de TI, responsável pelo serviço de correio eletrónico reserva-se o direito de bloquear o correio eletrónico que seja considerado impróprio e que não cumpra com as políticas e normas em vigor no Município de Alvaiázere.

Artigo 88.º - Exceções

Exceções a qualquer das normas desta secção, ou aos seus procedimentos, quando permitidas, devem ser aprovadas pela CSI.

Artigo 89.º - Responsabilização dos colaboradores

1. É da exclusiva responsabilidade do colaborador utilizador de correio eletrónico do município a sua correta utilização de acordo com as instruções e regras em vigor no Município de Alvaiázere;
2. Os colaboradores que detetem uma violação a qualquer uma das regras enunciadas anteriormente deverão comunicá-la, de imediato, ao respetivo superior hierárquico ou ao serviço de TI do Município de Alvaiázere;
3. A utilização incorreta do correio eletrónico dá lugar ao cancelamento da conta de correio e a processo disciplinar.

SECÇÃO X - Acesso à Internet

Artigo 90.º - Acesso à Internet

1. Todos os acessos aos serviços de Internet, exceto os que tecnicamente não permitam, são efetuados de forma centralizada através de um sistema de controlo de acessos WEB (ex: *firewall*);
2. Os acessos à Internet a partir da rede informática e terminais do Município de Alvaiázere têm de ser formalmente aprovados pelos dirigentes das respetivas áreas, que se responsabilizam pela concessão dos acessos em causa como necessários ao desempenho das atividades correntes dos seus colaboradores ou de entidades externas pelas quais sejam responsáveis;
3. O acesso à Internet destina-se a ser utilizado pelos colaboradores no âmbito das atividades profissionais contratadas pelo Município de Alvaiázere;
4. A utilização do acesso à Internet para uso pessoal, a título ocasional e preferencialmente fora do horário de trabalho, é admitida nas seguintes condições:
    a) quando não interfira com as respetivas atividades profissionais diárias;
    b) quando não prejudique, de algum modo, o Município de Alvaiázere e/ou os seus recursos;
    c) quando não ultrapasse/viole as restrições de conteúdos descritas nesta norma;
    d) quando não ocorra transferência de programas informáticos comerciais não licenciados ou de qualquer documento que refira proteção de propriedade (*Copyright*);
    e) quando não integre algum tipo de atividade ilegal.

Artigo 91º - Utilização correta dos recursos da Internet

1. Não é permitido utilizar a identificação de terceiros para obter acesso à Internet;
2. Os utilizadores não podem utilizar os seus privilégios de acesso à Internet para aceder, armazenar, processar ou imprimir material de natureza obscena, discriminatória, assediadora ou cujo conteúdo possa ofender terceiros com base na sua idade, sexo, raça, orientação sexual, credos políticos e religiosos, nacionalidade ou deficiência;
3. Não é permitido utilizar a Internet para solicitar um serviço privado para lucro ou ganho pessoal, para atividades ilegais, fraudulentas e/ou maliciosas;
4. É proibido efetuar atividades ilegais, incluindo jogo, *upload* ou *download* de *software* violando as leis de *copyright*;
5. Não é permitido aos colaboradores intencionalmente interferir com o *gateway* para a Internet do Município de Alvaiázere ou de qualquer outro site;
6. Não é permitido desativar, corromper ou de alguma forma contornar os sistemas de segurança implementados no acesso à Internet;
7. Não são permitidas tentativas de ganhar acesso não autorizado a outros sites;
8. Não é permitido utilizar a Internet para realizar atividade que seja contra a política de outras entidades, ou que possa ser contrária aos melhores interesses do Município de Alvaiázere;
9. Os colaboradores do Município de Alvaiázere não devem aceder a materiais de *streaming* que não estejam relacionados com a função, como é o caso de vídeo ou rádio pela Internet;
10. Não é permitido efetuar o *download* de ficheiros de áudio ou vídeo de qualquer tipo, quando não relacionados com a função;
11. Os colaboradores e as entidades externas que acedam à Internet a partir da rede informática e terminais do Município de Alvaiázere devem respeitar os direitos de propriedade intelectual e *copyright* aplicáveis aos conteúdos acedidos;
12. Não é permitido descarregar ou distribuir *software* de qualquer âmbito, sem que as licenças ou direitos de autor sejam respeitados.

Artigo 92º - Informação sensível

1. Não é permitido fornecer, pelo recurso ao acesso à Internet, informação classificada como confidencial ou de uso interno a pessoas não autorizadas;
2. Não é permitido usar o Messenger ou serviços semelhantes para divulgar informação confidencial ou de uso interno a pessoas fora da rede do Município de Alvaiázere;
3. A participação em *chat-rooms* ou fóruns de discussão é desaconselhada. Se tal participação for absolutamente necessária, deverá existir um cuidado especial em não divulgar informação confidencial ou de uso interno da organização.

Artigo 93º - Segurança das *passwords* de acesso

Não é permitido aos colaboradores do Município de Alvaiázere partilhar *passwords* de acesso, credenciais de acesso ou qualquer outro tipo de identificação pessoal pela Internet.

Artigo 94º - Administração, auditoria e monitorização

1. O Município de Alvaiázere reserva-se o direito de, numa filosofia preventiva, restringir o acesso à Internet a partir da sua rede informática e terminais, através da aplicação de filtros que impossibilitem, à partida, a visita e a navegação de *websites* eventualmente não autorizados pelo município;
2. Os acessos aos sites fora do município serão auditados e controlados através de equipamentos de segurança de perímetro;
3. Caso existam evidências de acessos que não cumpram com o estipulado no presente regulamento, poderão ser alvo de análise e avaliação pelo serviço de TI ou entidade nomeada para o efeito.

Artigo 95º - Exceções

Exceções a qualquer dos preceitos desta secção ou aos seus procedimentos, quando permitidas, devem ser aprovadas por escrito pela CSI.

Artigo 96º - Responsabilização dos colaboradores

1. Os colaboradores destinatários das normas dispostas nesta secção são responsáveis pelo seu cumprimento;
2. Os colaboradores que detetem uma violação a qualquer uma das normas desta secção deverão comunicá-la de imediato ao seu superior hierárquico ou ao serviço de TI;
3. A utilização incorreta do acesso à Internet poderá dar lugar ao cancelamento do mesmo, sem prejuízo das consequências disciplinares que daí possam advir.

SECÇÃO XI - Política de acesso remoto e dispositivos de acesso móvel

Artigo 97.º - Acesso remoto

1. A CSI deve proceder à análise dos riscos para determinar que tipos de controlos de segurança de informação são necessários para quem trabalha a partir de casa ou remotamente;
2. Devem ser implementadas medidas de segurança de informação específicas para quem trabalha a partir de casa, decorrentes de análise de risco prévia;
3. Devem ser implementados controlos de acesso nos computadores usados por quem trabalha a partir de casa;
4. Devem ser estabelecidas ligações seguras nas comunicações entre quem trabalha a partir de casa e dos escritórios;
5. Sempre que possível, o acesso remoto deve ser efetuado através de canais de acesso seguros controlados pelo Município de Alvaiázere, como é o caso de acesso VPN disponibilizado pela firewall;
6. Só é autorizado o acesso remoto a computadores portáteis que pertençam ao município e sob gestão do serviço de TI;
7. É proibida a utilização de computadores pessoais para acesso aos serviços do município, exceto quando autorizado pela CSI e sob gestão, controlo e monitorização do serviço de TI, nomeadamente análise ao computador antes de este ser ligado via VPN para análise de *malware*, antivírus atualizado, atualizações de segurança do sistema operativo e aplicações, análise ao *software* instalado, entre outros procedimentos internos ao serviço de TI.

Artigo 98.º - Acesso VPN

1. É da responsabilidade dos colaboradores ou entidades externas com privilégios de acesso VPN não permitir o acesso à rede do Município de Alvaiázere a utilizadores não autorizados;
2. O acesso à VPN do Município de Alvaiázere deve ser controlado por um método de autenticação forte (ex. *tokens*, *one-time-password*, sistema de chaves criptográficas, etc.);
3. Quando é estabelecida uma ligação VPN não deve ser permitida outra ligação de rede ativa no mesmo equipamento;
4. Todos os computadores ligados à rede interna do Município de Alvaiázere via VPN, incluindo computadores pessoais, devem ter o *software* de antivírus autorizado pelo Município de Alvaiázere instalado e atualizado;
5. Os utilizadores que estejam ligados via VPN são desligados automaticamente após 10 minutos de inatividade;
6. Ao utilizar a tecnologia VPN a partir de equipamentos pessoais, os utilizadores devem entender que os seus computadores são de facto uma extensão da rede do Município de Alvaiázere e, como tal, estão sujeitos às mesmas regras e regulamentações que se aplicam aos equipamentos propriedade do Município de Alvaiázere;
7. O serviço de TI deve possuir sempre uma lista atualizada de utilizadores com acesso VPN autorizados (Anexo III);
8. Os utilizadores a quem é disponibilizado o acesso VPN deverão ser informados das boas práticas a ter em conta na sua utilização (Anexo IV).

Artigo 99.º - Dispositivos de acesso móvel

1. Os colaboradores e entidades externas só podem utilizar dispositivos de acesso móvel (computadores portáteis, *smartphones*, tablets, etc.) para aceder aos sistemas e informação do Município de Alvaiázere quando devidamente autorizados pela CSI e com as devidas salvaguardas de segurança;
2. Em viagem, os computadores portáteis devem ser tratados como a bagagem de mão e deve-se assegurar que estão escondidos ou disfarçados;

3. Não devem ser armazenados dados considerados sensíveis em dispositivos móveis como disco externo, pen USB, etc., a não ser que sejam protegidos por mecanismos de encriptação aprovados pela CSI (ex: BitLocker Drive Encryption da Microsoft);
4. A utilização para fins pessoais de dispositivos móveis atribuídos pelo município deve ser reduzida e nunca deve comprometer a segurança do dispositivo e a confidencialidade e integridade da informação armazenada no mesmo;
5. O roubo ou comprometimento de qualquer dispositivo de acesso móvel com dados do Município de Alvaiázere deve ser imediatamente reportado.

Artigo 100.º - Responsabilização dos colaboradores

1. Os colaboradores e entidades externas com acesso remoto ao Município de Alvaiázere ou que utilizam dispositivos de acesso móvel, corporativos ou pessoais para aceder aos sistemas ou informação do Município de Alvaiázere são responsáveis pela sua correta utilização de acordo com as instruções em vigor no Município de Alvaiázere, dispostas no presente regulamento;
2. Os colaboradores que detetem uma violação a qualquer uma das normas enunciadas anteriormente deverão comunicá-la de imediato ao seu superior hierárquico ou ao serviço de TI;
3. A utilização incorreta dos acessos remotos ou dos dispositivos de acesso móvel do Município de Alvaiázere poderá dar lugar ao cancelamento dos mesmos, sem prejuízo das consequências disciplinares que daí possam resultar.

CAPÍTULO IV - Política de Ativos

Artigo 101.º - Entrega de ativo

O documento de Entrega & Devolução de Ativo (Anexo V) deve ser assinado no momento da entrega por quem recebe o ativo, devendo ter-se em consideração o seguinte:

a) no caso dos ativos se destinarem ao uso coletivo, deverá ser o dirigente do serviço a fazer a sua receção, mencionando-se esse facto nas observações;
b) um ativo cuja utilização seja maioritariamente de um único utilizador deve ser classificado como individual.

Artigo 102.º - Devolução de ativo

O documento de Entrega & Devolução de Ativo (Anexo V) deve ser assinado no momento da devolução do ativo pelo técnico que o receber.

CAPÍTULO V – Disposições finais

Artigo 103.º - Atualizações

1. A atualização da Política de Segurança e a comunicação dessa atualização aos seus colaboradores, às entidades externas e aos fornecedores é da responsabilidade da Câmara Municipal de Alvaiázere.
2. Os Anexos I, II, III, IV e V poderão ser objeto de alteração por decisão do Presidente da Câmara, ou do Vereador com competência delegada, sendo tal alteração comunicada em tempo útil aos colaboradores, às entidades externas e aos fornecedores.

Artigo 104.º - Dúvidas e omissões

Os casos omissos e as dúvidas suscitadas pela interpretação e aplicação do presente regulamento que não possam ser sanadas pelo recurso aos critérios legais de interpretação e integração de lacunas serão submetidas para decisão dos órgãos competentes.

Artigo 105.º - Entrada em vigor

O presente regulamento entra em vigor 15 dias após a sua publicação no *Diário da República*.

Anexo I

Entrega de *Password*

Utilizador (*username*)	
Email (profissional)	
Password (provisória)	

Deve alterar a *password* provisória no primeiro login no sistema.

As regras de composição das passwords:

a) Ter um tamanho mínimo de 8 caracteres;
b) Têm de conter caracteres de pelo menos 2 das seguintes categorias:
   i. Letras maiúsculas (A – Z);
   ii. Letras minúsculas (a – z);
   iii. Números (0 – 9);
   iv. Caracteres não alfanuméricos (por exemplo % $?);

Não é permitido pelo sistema que as *passwords* sejam iguais ao nome do utilizador;

Deve ter os três primeiros caracteres diferentes do identificador;

Deve ter os três primeiros caracteres diferentes entre si;

Não deve ter espaços na sua composição.

As *passwords* atribuídas aos utilizadores no âmbito de um dado sistema devem expirar automaticamente a cada 120 dias, obrigando à respetiva alteração;

Sempre que permitido tecnicamente pelo sistema, as *passwords* não podem ser reutilizadas por um mesmo utilizador antes de 5 iterações.

Anexo II

Email a enviar a todos os colaboradores do Município de Alvaiázere sobre a comunicação de incidentes de segurança informática

Comunicação de incidentes de segurança informática

Para:

Utilizadores da rede informática do Município de Alvaiázere

O Sistema de Gestão de Segurança de Informação considera que o correto tratamento de incidentes de segurança constitui-se numa aprendizagem, permitindo melhorar os controlos implementados e, assim, reduzir a frequência, os danos e os custos potenciais de futuros incidentes. Em consequência, o referido Sistema obriga à definição de uma norma específica que sistematiza o tratamento dos incidentes verificados, através de um processo próprio.

Um incidente de segurança informática pode definir-se como:

- Um acesso, tentativa de acesso, uso, divulgação, modificação ou destruição não autorizada de informação;
- Um impedimento do funcionamento normal das redes, sistemas ou recursos informáticos;
- Uma violação ou ameaça eminente à Política de Segurança de Informação da Câmara Municipal de Alvaiázere.

Como exemplo de incidentes de segurança informática podemos enumerar:

- Acesso não autorizado ou obtenção indevido de passwords;
- Obtenção, divulgação, alteração ou destruição indevida de informação;
- Interrupção persistente de um serviço ou programa (p.e. email, internet, *sign-on*, portais, ERP, etc.);
- Qualquer vulnerabilidade (fraqueza nos sistemas de proteção) observada ou suspeita.

A comunicação dos incidentes ocorridos é, portanto, o primeiro passo neste processo.

Assim, solicita-se a todos os utilizadores da rede informática do Município de Alvaiázere que reportem os incidentes de segurança de informação que venham a observar. Esta comunicação deve ser participada ao Serviço de TI, verbal ou telefonicamente, ou ainda por email, utilizando o endereço XXX@cm-alvaiazere.pt, através do qual pode também ser pedido qualquer esclarecimento.

A obtenção e manutenção de um elevado nível de segurança dos sistemas informáticos é uma responsabilidade partilhada, pelo que estamos certos da colaboração solicitada.

Anexo III

Lista de utilizadores autorizados a ligações VPN

Utilizador	User ID	Serviço	Perfil

Anexo IV

Acesso VPN: melhores práticas de utilização

Na cultura atual de mobilidade, cada vez mais os colaboradores e parceiros acedem aos serviços das organizações de locais remotos, quer seja em casa, quer seja de qualquer outro local, a partir dos seus computadores pessoais e de dispositivos móveis como *smartphone*, entre outros.

O problema dos acessos remotos e do acesso a partir de dispositivos de acesso móvel é que, muitas vezes, nem o dispositivo nem a rede são controlados pelo município, pelo que os riscos de segurança são muito mais elevados que aqueles que estão associados aos acessos normais a partir dos equipamentos instalados no município.

O objetivo deste documento é informar os colaboradores e entidades externas, enquanto prestadoras de serviço, dos cuidados a ter em conta nos acessos remotos aos sistemas da Município de Alvaiázere, com vista a proteger este tipo de ligação que, por defeito, está mais exposto a riscos de segurança.

Assim, recomenda-se que:

a) Se utilize a ligação VPN preferencialmente em equipamentos fornecidos pela instituição;
b) Quando for estabelecida uma ligação VPN não seja efetuada outra ligação de rede ativa no mesmo equipamento;
c) Os computadores nos quais se utilizam ligações VPN devem ter o antivírus atualizado e as atualizações criticas de segurança instaladas, bem como deve existir um cuidado adicional na seleção das aplicações a instalar;
d) Se utilize o WebMail em detrimento da ligação VPN, se se pretende apenas aceder ao Outlook;
e) Se configure uma *pre-shared key* em redes domésticas. Muitos *routers* wireless utilizados em casa não estão configurados com a segurança adequada;
f) Cuidados adicionais devem ser tidos em conta quando a ligação à Internet é estabelecida em locais públicos (ex: aeroportos, hotéis, etc.) onde as redes são partilhadas e por isso utilizadas por outros utilizadores pouco cientes de implicações de segurança;
g) Não devem ser armazenados dados do município em dispositivos móveis, como disco externo, pen, etc., a não ser que sejam protegidos por mecanismos de encriptação (ex: BitLocker Drive Encryption da Microsoft, disponível no Windows);
h) O roubo ou comprometimento de qualquer dispositivo de acesso móvel com dados do Município de Alvaiázere deverá ser imediatamente reportado.

Finalmente, ao utilizar a tecnologia VPN a partir de equipamentos móveis, os utilizadores devem entender que os seus equipamentos são de facto uma extensão da rede do Município de Alvaiázere e, como tal, estão sujeitos às mesmas regras e regulamentações que se aplicam aos equipamentos instalados e utilizados nas instalações do município.

Para o esclarecimento de qualquer dúvida pode contactar o serviço de TI.

Anexo V

Entrega & Devolução de Ativo

ID do Ativo	Descrição (marca, modelo, etc.)

Nº. de Série	Tipo (portátil, desktop, etc.)	Uso (individual, coletivo)

Data de entrega	Nome

Observações	Recebi
	_____

É da responsabilidade dos Utilizadores manter os equipamentos em bom estado de conservação.

Data	**Registo de Alterações**
/ /	
/ /	
/ /	
/ /	

Observações	**Devolução**
	_____