MUNICÍPIO DE MIRA

Aviso n.º 1813/2023

Sumário: Aprova o Regulamento Municipal de Segurança da Informação.

Raul José Rei Soares de Almeida, presidente da Câmara Municipal de Mira, faz público, em cumprimento do disposto no artigo 139.º do Código de Procedimento Administrativo, que a Câmara Municipal, em reunião ordinária de 7 de dezembro de 2022, e a Assembleia Municipal, em sessão ordinária de 16 de dezembro de 2022, deliberaram, por unanimidade, aprovar, dispensando a fase de audiência dos interessados, o Regulamento Municipal de Segurança da Informação, que entrará em vigor 15 dias após a sua publicação no *Diário da República.*

Para constar e devidos efeitos se publica o presente aviso e o referido Regulamento no *Diário da República* e vão ser divulgados no sítio do Município de Mira, em www.cm-mira.pt, e nos locais de estilo.

21 de dezembro de 2022. — O Presidente da Câmara Municipal, *Raul José Rei Soares de Almeida*.

Regulamento Municipal de Segurança da Informação

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 Mira; 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, o Decreto-Lei n.º 65/2021, de 30 julho que regulamenta 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 14.º do Código do Procedimento Administrativo.

Destarte, cabe ao Município de Mira 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.

Decorrido o procedimento de elaboração previsto na lei, sob proposta da Câmara Municipal, a Assembleia Municipal de Mira aprova, sob a forma de regulamento, o Regulamento Municipal de Segurança de Informação.

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.

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, do artigo 14.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança no ciberespaço, conjugado com o artigo 14.º do Código do Procedimento Administrativo, na sua redação atual e do artigo 7.º do Decreto-Lei n.º 65/2021 de 30 de julho.

Artigo 2.º

Objetivos da política de segurança de informação

1 — A segurança da informação tem como principais objetivos garantir os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade, requeridos para a sua proteção, mitigando assim o impacto de eventuais incidentes que possam comprometer o regular funcionamento do Município de Mira.

2 — A integridade consiste na capacidade de prevenir, recuperar e reverter alterações não autorizadas ou acidentais aos dados.

3 — A autenticidade consiste na manutenção da fiabilidade da informação desde o momento da sua produção e ao longo de todo o seu ciclo de vida.

4 — A disponibilidade refere-se à possibilidade de acesso aos dados, quando necessário.

5 — A confidencialidade refere-se à capacidade de proteger os dados daqueles que não estão autorizados a consultá-los, não impedindo o acesso aos mesmos, em tempo útil, de pessoas autorizadas.

6 — As disposições do presente regulamento são aplicáveis a todos órgãos, serviços e organismos municipais do Município de Mira, designadamente membros do executivo, dos trabalhadores, bem como prestadores de serviços externos e entidades que utilizam as instalações e meios do

Município de Mira, às entidades externas que exerçam competências municipais em regime de delegação de competências e às demais entidades externas relevantes.

7 — Além do acesso adequado à informação necessária para o desempenho das suas funções, todos os utilizadores devem ter conhecimento deste regulamento sendo-lhes exigido o respeito pelos controlos de segurança implementados.

8 — Para o cumprimento destes objetivos, o Município de Mira, em conformidade com a legislação e normativos em vigor em matéria de segurança da informação, compromete-se a adotar as melhores práticas nacionais e internacionais.

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;
SRH: Secção de Recursos Humanos;
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
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 entre outros no Windows 10 e Windows 11. 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 Mira;

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 Mira. 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 Mira, 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 Edge) 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 Mira.

2 — É da responsabilidade do Município de Mira 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 Mira são responsáveis por garantir e manter as políticas, normas e controlos de segurança de informação definidos pela respetiva chefia.

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 Mira e entidades externas com acesso à informação são responsáveis tanto pela sua proteção como utilização.

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 Mira.

3 — Todos os parceiros de serviço, fornecedores e clientes do Município de Mira de- vem 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 Mira.

Artigo 10.º

Âmbito de atuação

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;

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 Mira.

Artigo 11.º

Estrutura

A Comissão de Segurança de Informação é composta por:

a) Presidente da Comissão de Segurança;
b) Vice-Presidente da Comissão de Segurança;
c) Computer Operations Manager (COM);
d) Gabinete de Planeamento Estratégico, Qualidade e Auditoria (GPEQA);
e) Representante de todas as Divisões e Unidades Orgânicas do Município.

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 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

Auditoria Interna

A Auditoria Interna 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

Computer Operations Manager (COM)

O COM, está integrado no serviço de informática e:

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 informática, de modo que a integridade, disponibilidade e segurança dos sistemas de informação sejam mantidos;

d) Mantém 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 informática;

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 informática.

Artigo 15.º

Serviço Jurídico

A CSI pode solicitar a colaboração da área de Contratação Pública, Assessoria e Jurídico para a validação da conformidade legal da Segurança de Informação no Município de Mira.

Artigo 16.º

Secção de Recursos Humanos

A CSI define, em colaboração com a Divisão Administrativa e Financeira, as ações a desencadear para a sensibilização dos colaboradores do Município de Mira para as questões de segurança da informação.

SECÇÃO III

Política de Organização Externa e Interna

Artigo 17.º

Organização externa

1 — O serviço de informática 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 Mira.

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 informática, a solicitação de um serviço.

5 — Atividades que tenham como requisito os acessos 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 18.º

Acordos de confidencialidade

1 — Todas as entidades externas que contenham informação da organização assinam um acordo de confidencialidade com o Município de Mira, 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 19.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 informática, 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 20.º

Uso do nome da instituição por parceiros externos

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

Artigo 21.º

Tratamento da informação corporativa no término de contratos

1 — Se o Município de Mira 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 22.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 Mira.

Artigo 23.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 24.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 Mira.

Artigo 25.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 26.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 27.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 Mira.

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 28.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 Mira, internos e externos, e devidamente se- lecionados 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 29.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 Mira.

Artigo 30.º

Controlos de novas tecnologias

1 — Em todos os casos onde se possa utilizar novas tecnologias nos sistemas produtivos do Município de Mira, 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 31.º

Paragem de componentes de segurança críticos

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

Artigo 32.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

Artigo 33.º

Âmbito

Os sistemas informáticos têm um papel cada vez mais importante numa instituição. A sua gestão de acessos e a sua crescente complexidade requerem uma constante monitorização de forma a garantir um sistema seguro, fiável, robusto e de alta produtividade. Os resultados dessa monitorização são informação imprescindível para uma constante proteção e evolução.

Os princípios deste capítulo estão descritos na Política Complementar deste Regulamento.

CAPÍTULO IV

Política de Ativos

Artigo 34.º

Entrega de ativo

O documento de Entrega e 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 35.º

Devolução de ativo

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

CAPÍTULO V

Disposições finais

Artigo 36.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 Mira;

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 37.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 deliberação da Câmara Municipal.

Artigo 38.º

Entrada em vigor

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

ANEXOS

ANEXO I

Entrega de *Password*

Município de Mira

Nome:

Utilizador:

E-mail Profissional:

Password (provisória):

ANEXO II

***E-mail* a enviar a todos os colaboradores do Município de Mira sobre a comunicação de incidentes de segurança informática**

Comunicação de incidentes de segurança informática

Para:

Utilizadores da rede informática do Município de Mira

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:

a) Um acesso, tentativa de acesso, uso, divulgação, modificação ou destruição não autorizada de informação;

b) Um impedimento do funcionamento normal das redes, sistemas ou recursos informáticos;

c) Uma violação ou ameaça eminente à Política de Segurança de Informação da Câmara Municipal de Mira.

Como exemplo de incidentes de segurança informática podemos enumerar:

a) Acesso não autorizado ou obtenção indevida de passwords;
b) Obtenção, divulgação, alteração ou destruição indevida de informação;
c) 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 Mira que reportem os incidentes de segurança de informação que venham a observar. Esta comunicação deve ser participada ao Serviço de informática, verbal ou telefonicamente, ou ainda por *email*, utilizando o endereço suporte@cm-mira.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

Nome	Utilizador	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 Mira, 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 críticas de segurança instaladas, bem como deve existir um cuidado adicional na seleção das aplicações a instalar;
d) Se configure uma pre-shared key em redes domésticas. Muitos routers wireless utilizados em casa não estão configurados com a segurança adequada;
e) 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;

f) 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;

g) O roubo ou comprometimento de qualquer dispositivo de acesso móvel com dados do Município de Mira 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 Mira 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 informática.

ANEXO V

Entrega e devolução de Ativo

MUNICÍPIO DE **mira**
DIVISÃO ADMINISTRATIVA E FINANCEIRA

termo de entrega

DECLARAÇÃO

Eu, [**nome**], a desempenhar funções no Município de Mira, declaro que em [**data**] entreguei / recebi a / de (1) [**nome do que recebeu ou facultou**] os equipamentos abaixo indicados, fornecidos para o exercício das minhas funções neste Município.

1. [**Equipamento**]

Observações:

[**Local, data**]

O Trabalhador
[**Nome do trabalhador**]

O Trabalhador que recebeu ou facultou o equipamento

_____

[**Nome do trabalhador**]

(1) – Riscar o que não interessa

É da responsabilidade do utilizador manter os equipamentos em bom estado de conservação.

315995674