CONCURSO PÚBLICO, SEM PUBLICAÇÃO DE ANÚNCIO NO JOUE, PARA AQUISIÇÃO DE SERVIÇOS DE ENCARREGADO DE PROTEÇÃO DE DADOS (EPD) E DE SERVIÇOS ESPECIALIZADOS, POR EQUIPA MULTIDISCIPLINAR, PARA APOIO À GESTÃO DO SISTEMA DE PROTEÇÃO DE DADOS DO MUNICÍPIO DA AMADORA

CADERNO DE ENCARGOS

ÍNDICE

PARTE I – CLÁUSULAS JURÍDICAS

PARTE II – CLÁUSULAS TÉCNICAS

ANEXOS:

PARTE I

Cláusulas jurídicas

Cláusula 1.ª

Objeto

O objeto do contrato consiste na prestação de serviços de Encarregado de Proteção de Dados (EPD) e de serviços especializados, por equipa multidisciplinar, para apoio à gestão do sistema de proteção de dados do Município da Amadora, de acordo com as cláusulas técnicas constantes da parte II do presente caderno de encargos.

Cláusula 2.ª

Preço base

1 - O preço base (*"preço máximo")* do contrato a celebrar é de **65.700,00 €,** acrescido do IVA à taxa legal em vigor.

2 – O preço base indicado no número anterior foi estabelecido na sequência de consulta preliminar ao mercado nos termos previstos na cláusula 3.ª do presente caderno de encargos.

Cláusula 3.ª

Consulta preliminar ao mercado

Nos termos do disposto nos artigos 47.º, n.º 3 e 35.º - A, ambos do Código dos Contratos Públicos (CCP), previamente ao presente procedimento foi efetuada consulta preliminar ao mercado, sendo que o preço base mencionado na cláusula anterior foi fixado com base na multiplicação dos preços médios unitários, constantes dos orçamentos obtidos nesta sede, pelo período de vigência do contrato a celebrar (36 meses).

Cláusula 4.ª

Local da prestação de serviços

Os serviços objeto do presente contrato serão prestados nas instalações do cocontratante e nos serviços da entidade adjudicante, nos termos previstos do n.º 3 do ponto 2 da Parte II - Cláusula técnicas do presente caderno de encargos.

Cláusula 5.ª

Prazo de vigência do contrato

1- O contrato produzirá efeitos desde a data da sua assinatura, sendo os serviços objeto do mesmo prestados por um período de 36 meses, com inicio em 1 de junho de 2026 e terminus a 30 de maio de 2029.

2 - Sem prejuízo do disposto no número anterior, o contrato poderá começar a produzir os seus efeitos depois de 1 de junho de 2026 caso a data da adjudicação, habilitação do adjudicatário, ou qualquer outro evento, não permita a celebração do contrato antes dessa data, caso em que o início da vigência ocorrerá a partir da data da respetiva assinatura e o terminus 36 (trinta e seis) meses depois dessa data.

Cláusula 6.ª

Condições de pagamento

1- O preço contratual será pago em 36 (trinta e seis) prestações mensais, iguais e sucessivas, devendo o cocontratante remeter, ao contraente público a respetiva fatura, nos termos dos números seguintes.

2 - A entidade adjudicante só efetuará os pagamentos depois de comprovada a efetiva prestação de serviços a que diz respeito.

3 - Para efeitos do número anterior, o cocontratante fica obrigado a enviar à entidade adjudicante, até ao 5.º dia de cada mês, um relatório de execução referente aos trabalhos desenvolvidos no mês transato, para efeitos de validação pelo gestor do contrato.

4 - O gestor do contrato dispõe de 5 dias para validar o relatório de execução enviado pelo cocontratante. Em caso de discordância, rejeita a validação do mesmo de forma devidamente fundamentada ou solicita documentação e prova adicional do cumprimento, dispondo o cocontratante, neste último caso, de 5 dias para remeter a informação e/ou documentação adicional necessária.

5 - Depois de obtida a validação do relatório de execução por parte do gestor do contrato, pode o cocontratante emitir fatura no valor da prestação de serviços, referente ao mês em causa, devendo o pagamento ocorrer no prazo de 30 dias.

6 - Nas são permitidos adiantamentos por conta dos serviços a prestar.

Cláusula 7.ª

Equipa a afetar à execução das prestações contratuais

1- A equipa multidisciplinar a afetar à execução do contrato é a indicada pelo cocontratante na sua proposta, e deve apresentar elementos com todas as valências requeridas nas especificações técnicas, nomeadamente ao nível jurídico, de gestão e técnico para assegurar as funções de EPD, diagnosticar a maturidade do sistema, apoiar a gestão do sistema de proteção de dados, apoio à realização de auditorias e sessões de sensibilização, garantindo a conformidade com o RGPD e a articulação com a cibersegurança municipal.

2 - Esta equipa deve cumprir efetivamente as especificações de qualidade previstas no caderno de encargos e nos requisitos técnicos exigidos.

3 - Caso, durante a execução do contrato, se constate que a equipa não apresenta valências nem competências adequadas à execução do contrato, o contraente público pode ordenar a alteração de um ou mais elementos da equipa ao cocontratante de forma devidamente fundamentada.

4 - Caso se aplique o previsto no número anterior, o cocontratante dispõe de 10 dias para enviar ao contraente público proposta de elemento ou elementos a integrar a equipa, fazendo acompanhar essa proposta dos respetivos curriculum vitae e certificados de formação no âmbito do RGPD. Em todo o caso, os novos elementos só integram a equipa mediante autorização expressa do contraente público.

5 - Caso o cocontratante pretenda, em sede de execução do contrato, substituir um ou mais elementos da equipa apresentada em sede de proposta, o(s) novo(s) elemento(s) proposto(s) pelo adjudicatário só pode(rão) integrar a equipa com o expresso e prévio consentimento da entidade adjudicante, após verificação de que essa substituição proporciona um

nível de qualidade equivalente, devendo o cocontratante apresentar na sua proposta de substituição os curriculum vitae e certificados de formação no âmbito do RGPD dos novos elementos propostos.

Cláusula 8.ª

Gestor do contrato

Nos termos do disposto no artigo 290.ºA, conjugado com o artigo 96.º, n.º1 alínea i), ambos do Código dos Contratos Públicos, as funções de gestor do contrato serão desempenhadas pela Dra. Teresa Pinheiro, Técnica Superior do GMF/DMTIC do Município da Amadora.

Cláusula 9.ª

Sigilo

O cocontratante garantirá o sigilo quanto a informações que os seus técnicos venham a ter conhecimento relacionadas com a atividade do contraente público.

Cláusula 10.ª

Cessão da posição contratual

Em caso de incumprimento do contrato, poderá ser aplicado o disposto no artigo 318.º-A do CCP.

Cláusula 11.ª

Penalidades contratuais

1- No caso de incumprimento das obrigações previstas no presente caderno de encargos, por causa imputável ao cocontratante, este ficará sujeito ao pagamento de multa correspondente até 1% sobre o preço total da prestação de serviços, por cada incumprimento, a determinar em função da gravidade e consequências do mesmo.

2 - O gestor do contrato, em caso de incumprimento, poderá elaborar o enquadramento dos factos, enquadramento contratual e valor previsível da penalidade, e notificar o cocontratante para o exercício de audiência prévia por um período de 10 dias. Findo esse prazo e depois de ponderada a pronúncia apresentada, o gestor do contrato pode propor ao órgão competente do contraente público a aplicação de penalidades.

3 - As penalidades, quando aplicadas, serão deduzidas na faturação mensal.

Cláusula 12.ª

Casos fortuitos ou de força maior

1 - Nenhuma das partes incorrerá em responsabilidade se por caso fortuito ou de força maior, designadamente greves ou outros conflitos de trabalho, for impedido de cumprir as obrigações assumidas no contrato.

2 - A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

Cláusula 13.ª

Patentes, licenças e marcas registadas

1 - São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.

2 - Caso o contraente público venha a ser demandado por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o cocontratante indemniza-o de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.

Cláusula 14.ª

Resolução do contrato pelo contraente público

Sem prejuízo das causas de resolução previstas na lei e da aplicação das penalidades legal e contratualmente previstas, o contrato poderá ser unilateralmente resolvido pelo contraente público no caso de se verificar um incumprimento grave e reiterado das obrigações previstas no caderno de encargos relativas à execução da prestação de serviços, que tenha como consequência o incumprimento de obrigações decorrentes do Regulamento Geral sobre a Proteção de Dados, em pelo menos uma ocorrência.

Cláusula 15.ª

Tratamento de dados pessoais

1 – Nos termos e para os efeitos previstos no Regulamento Geral de Proteção de Dados (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, os eventuais dados pessoais que venham a ser transmitidos no presente procedimento serão tratados com a finalidade de gestão e conclusão daquele, ou para outras finalidades que decorram de obrigações legais a que o contraente público esteja adstrito.

2 – Todos os dados pessoais que vierem a figurar no contrato a celebrar serão tratados com a finalidade de formação e execução da relação contratual, ou para outras finalidades que decorram de obrigações legais a que o contraente público esteja adstrito.

Cláusula 16.ª

Foro competente

O foro competente para dirimir quaisquer conflitos decorrentes do presente contrato é o do tribunal administrativo que tenha jurisdição sobre o Município da Amadora.

PARTE II
Cláusulas técnicas

1. Objeto do contrato a celebrar

O contrato a celebrar tem por objeto a prestação de serviços de Encarregado de Proteção de Dados (doravante designado por EPD) e de serviços especializados, por equipa multidisciplinar, para apoio à gestão do sistema de proteção de dados do Município da Amadora.

O Regulamento (UE) 2016/679 - Regulamento Geral sobre a Proteção de Dados (doravante designado RGPD) define as entidades que estão obrigadas a designar um EPD, bem como as suas funções.

O Município da Amadora enquanto organismo público, tem obrigatoriamente de nomear um EPD, nos termos da alínea a), do n.º 1, do Artigo 37º. do RGPD.

Ainda de acordo com o estabelecido no n.º 5 do artigo 37.º do RGPD, o encarregado de proteção de dados (EPD) deve ser, obrigatoriamente, detentor de conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como, deter capacidade para desempenhar as funções referidas no artigo 39.º do RGPD.

2. Funções do EPD e do cocontratante:

1. De acordo com o estabelecido no n.º 1 do artigo 39.º do RGPD, o EPD tem, pelo menos, as seguintes funções:

- Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;
- Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
- Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35º do regulamento;
- Coopera com a autoridade de controlo;
- Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36 º do Regulamento, e consulta, sendo caso disso, esta autoridade sobre qualquer outFaudro assunto;
- No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

2. Por força das funções acima descritas, o Cocontratante fica obrigado a afetar uma equipa multidisciplinar à realização específica das seguintes tarefas/atividades:

- Identificação do estado de maturidade na implementação do Regulamento;

- Identificação dos serviços a intervencionar com definição de grau de prioridade com base no levantamento inicial identificado no ponto anterior, relevando os pontos sensíveis ou não conformidades detetadas e propostas de medidas a implementar;
- Identificação dos entregáveis/resultados a apresentar, nomeadamente relatórios de diagnóstico, de acompanhamento/monitorização de implementação de medidas;
- Documentos de suporte à decisão do Responsável pelo Tratamento e periodicidade dos mesmos;
- Identificação dos requisitos mínimos a apresentar pela entidade adjudicante, necessários à prossecução das funções de EPD;
- Apresentação de cronograma/plano de trabalhos;
- Sessões de esclarecimento/sensibilização aos serviços – 2 sessões a cada trimestre;
- Formação de auditores internos ou, em alternativa, orientações relativamente aos requisitos e competências do auditor interno;
- Apoio à gestão do sistema de proteção de dados nos diversos serviços do Município;
- Apoio à realização de auditorias com auditores internos;
- O Cocontratante compromete-se ainda a analisar e responder às questões que forem apresentadas pelos serviços da entidade adjudicante, no âmbito das suas competências e funções, no prazo máximo de 5 dias úteis, após a sua receção;
- Outras que considere necessárias à prossecução dos objetivos de implementação de um sistema de gestão de proteção de dados robusto e eficaz.

3. Modo de execução da prestação de serviços

1. O serviço a prestar será na modalidade de avença mensal, com obrigatoriedade de uma visita semanal, aos serviços da entidade adjudicante, em dia/horário a acordar com esta, e prestação de serviços equivalente a uma carga horária mensal de 35 horas.

2. Deverá ser salvaguardado o cumprimento de prazos legais de resposta a entidades diversas (ex: CNPD).

3. Deverá ainda cooperar/articular com a Comissão de Segurança da Informação da Câmara Municipal da Amadora (CSICMA) todas as matérias relacionadas com a segurança da informação e cibersegurança (despacho n.º 04/P/2025, de 28 de janeiro), com a Unidade orgânica (UO) responsável pela área da Formação e com o Gabinete de Auditoria e Controlo Interno.

4. Dever de sigilo e confidencialidade do EPD

De acordo com o disposto no n.º 5 do artigo 38.º do RGPD, o EPD está obrigado a um dever de sigilo ou de confidencialidade, em tudo o que diga respeito ao exercício dessas funções, que se mantém após o termo das funções que lhes deram origem. Para efeitos do disposto, o cocontratante deverá, logo após a assinatura do contrato, subscrever a declaração de confidencialidade para empresas prestadoras de serviços, de acordo com os requisitos de confidencialidade para proteção da informação da Câmara Municipal da Amadora, conforme documento junto como anexo I a este caderno de encargos.

Amadora,

PRESIDENTE

VITOR FERREIRA

Requisitos de Confidencialidade para Proteção da Informação da Câmara Municipal da Amadora

Informação Confidencial

Apresentam-se de seguida os requisitos de confidencialidade para a proteção de informação da Câmara Municipal da Amadora que tenha sido alvo de classificação como "Confidencial" e que devem incorporar todos os acordos de confidencialidade e não-divulgação de informação a estabelecer com terceiros prestadores de serviço para a CMA que se encontrem dento do âmbito do SGSI estabelecido e que acedam a esta nível de informação classificada:

Cláusula	Requisito
Definição de Informação Confidencial	Incorporar a definição de "Informação Confidencial" no contrato a estabelecer – ver texto após a presente tabela
Duração mínima do acordo de confidencialidade e não-divulgação de informação	Igual ao contrato de prestação de serviços estabelecido.
Validade após resolução contratual	A validade dos termos do acordo de confidencialidade e não-divulgação de informação permanece ativo nos 5 anos subsequentes à data da resolução contratual.
Devolução de informação Confidencial	Toda e qualquer informação confidencial da Câmara Municipal da Amadora em posse do signatário será devolvida a esta na data de resolução do contrato de prestação de serviços.
Proteção da Informação Confidencial	O signatário compromete-se a proteger adequadamente a informação confidencial a que tenha acesso, durante todo o seu ciclo de vida, adotando os controlos de segurança da informação instituídos pela Câmara Municipal da Amadora, quando nas instalações desta ou noutros locais externos a esta.
Propriedade Intelectual	Toda a informação considerada como "Propriedade Intelectual", produzida ao abrigo do contrato de serviços estabelecido, é propriedade exclusiva da Câmara Municipal da Amadora, permanecendo esta como sua propriedade após o término do contrato estabelecido.
Uso permitido da Informação confidencial	Não é permitida a utilização de informação confidencial da Câmara Municipal da Amadora para outros fins que não aqueles diretamente inerentes ao serviço contratado. O signatário não tem autorização para utilização de informação confidencial da Câmara Municipal da Amadora para outros fins sem a autorização expressa da CMA.
Direito de Auditar	É concedido o direito à Câmara Municipal da Amadora para auditar pessoas, processos, procedimentos e locais do signatário ou de outros por este subcontratados, quanto à conformidade dos níveis de proteção da informação confidencial da CMA que o signatário incorpora nas suas atividades.
Notificação de quebra de segurança da informação	O signatário é obrigado a, da forma mais expedita, comunicar ao Responsável de Segurança da Informação da Câmara Municipal da Amadora qualquer suspeita ou facto de compromisso de confidencialidade da informação confidencial da CMA.

Quebra do contrato de confidencialidade estabelecido	Caso o contrato de confidencialidade estabelecido seja quebrado por responsabilidade do signatário, a Câmara Municipal da Amadora abrirá de imediato um inquérito interno no sentido de apurar formalmente responsabilidades e sansões pecuniárias ou outras a inferir ao signatário. Cabe à Câmara Municipal da Amadora decidir quanto à suspensão ou resolução imediata do serviço contratado.
Responsabilidades e autoridades para com a Segurança da Informação	Incorporar as responsabilidades e autoridades inerentes a “Entidades externas utilizadoras do Sistema de Informação da CMA (terceiros fornecedores de serviços) ” e “Outros”.

Considera-se “Informação Confidencial”:

- Quaisquer dados ou conhecimentos que requerem que a sua utilização seja restrita a elementos pré-autorizados e que em caso de incidente de segurança, pode causar impactos substanciais na imagem, reputação ou confiança da CMA;

- Informação que contenha:
    - Dados Pessoais;
    - Dados de Saúde;
    - Dados sobre Meios de Pagamento ou suas transações;
    - Dados sob Propriedade Intelectual.

- Informação que esteja sujeita a medidas de proteção especial devido a requisitos legais ou contratuais.

Informação Interna

Apresentam-se de seguida os requisitos de confidencialidade para a proteção de informação da Câmara Municipal da Amadora que tenha sido alvo de classificação como “Interna” e que devem incorporar todos os contractos de confidencialidade e não-divulgação de informação a estabelecer com terceiros prestadores de serviço para a CMA que se encontrem dento do âmbito do SGSI estabelecido e que acedam a esta nível de informação classificada:

Cláusula	Requisito
Definição de Informação Interna	Incorporar a definição de “Informação Interna” no contrato a estabelecer – ver texto após a presente tabela
Duração mínima do contrato de confidencialidade e não-divulgação de informação	Igual ao contrato de prestação de serviços estabelecido.
Validade após resolução contratual	A validade dos termos do acordo de confidencialidade e não-divulgação de informação permanece ativo nos 12 meses subsequentes à data da resolução contratual.
Devolução de informação Confidencial	Toda e qualquer informação interna da Câmara Municipal da Amadora em posse do signatário será devolvida a esta entidade na data de resolução do contrato de prestação de serviços.

Proteção da Informação Interna	O signatário compromete-se a proteger adequadamente a informação interna a que tenha acesso, durante todo o seu ciclo de vida, adotando os controlos de segurança da informação instituídos pela Câmara Municipal da Amadora, quando nas instalações desta ou noutros locais externos a esta.
Propriedade Intelectual	Toda a informação considerada como "Propriedade Intelectual", produzida ao abrigo do contrato de serviços estabelecido, é propriedade exclusiva da Câmara Municipal da Amadora, permanecendo esta como sua propriedade após o término do contrato estabelecido.
Uso permitido da informação Interna	Não é permitida a utilização de informação interna da Câmara Municipal da Amadora para outros fins que não aqueles diretamente inerentes ao serviço contratado. O signatário não tem autorização para utilização de informação interna da Câmara Municipal da Amadora para outros fins sem a autorização expressa da CMA.
Direito de Auditar	É concedido o direito à Câmara Municipal da Amadora para auditar pessoas, processos, procedimentos e locais do signatário ou de outros por este subcontratados, quanto à conformidade dos níveis de proteção da informação interna da CMA que o signatário incorpora nas suas atividades.
Notificação de quebra de segurança da informação	O signatário é obrigado a, da forma mais expedita, comunicar ao Gestor de Segurança da Informação da Câmara Municipal da Amadora qualquer suspeita ou facto de compromisso de confidencialidade da informação interna da CMA.
Quebra do contrato de confidencialidade estabelecido	Caso o contrato de confidencialidade estabelecido seja quebrado por responsabilidade do signatário, a Câmara Municipal da Amadora abrirá de imediato um inquérito interno no sentido de apurar formalmente responsabilidades e sansões pecuniárias ou outras a inferir ao signatário. Cabe à Câmara Municipal da Amadora decidir quanto à suspensão ou resolução imediata do serviço contratado.

Considera-se "Informação Interna" quaisquer dados ou conhecimentos, não públicos ou confidenciais, de suporte às atividades da Câmara Municipal da Amadora.
Refª NP ISO/IEC 27001:2013 - §A.13.2.4

REQUISITOS DA SEGURANÇA DA INFORMAÇÃO

ÍNDICE

1. Considerações sobre especificação e análise de Requisitos da Segurança da Informação

Sempre que se inicie um processo de desenvolvimento de um novo sistema de informação devem ser identificados, documentados e revistos regularmente os Requisitos da Segurança da Informação utilizando diversos métodos nomeadamente derivar requisitos de conformidade face a políticas e regulamentação, modelação de ameaças ou revisões de incidentes da Segurança da Informação.

Os requisitos da Segurança da Informação e os controlos devem refletir o valor da informação para com o negócio e o potencial impacto negativo que poderá resultar pela proteção dessa informação de forma inadequada.

A identificação e a gestão dos Requisitos da Segurança da Informação e processos associados devem ser integrados nos estágios iniciais de projetos de novos sistemas de informação.

Os requisitos da Segurança da Informação para novos sistemas de informação devem considerar os seguintes vetores de análise:

- Autenticação, quanto ao nível de confiança requerido quanto à identidade dos utilizadores (User ID e password, autenticação por dois fatores, SSO, como exemplos);

- Autorização, quanto aos processos de autorização e provisionamento de utilizadores comuns bem como para utilizadores privilegiados e de serviço;

- Papéis, responsabilidades e segregação de funções, no que diz respeito à necessidade de informação de utilizadores e outras entidades envolvidas, quanto às suas responsabilidades para com o sistema e a sua informação, e à necessidade do assegurar da segregação das atividades desempenhadas;

- Confidencialidade, integridade e disponibilidade, quanto aos níveis de proteção dos ativos de informação e à utilização de técnicas de segurança como cifra, não-repúdio, autenticação de mensagens, assinaturas digitais, redundância e recuperação;

- Logs de auditoria e monitorização, quanto aos níveis de detalhe da informação a ser produzida pela utilização do sistema, seu local de salvaguarda e privilégios de acessos de utilizadores a esta informação.

2. Documentação de referência

- Norma ISO/IEC 27001:2013, §A.14.1; §A.14.2; §A.14.3
- Política da Segurança da Informação

3. Requisitos mínimos de segurança da informação para novos sistemas

No caso de aquisição de soluções ou aplicações a fornecedores externos, os requisitos a considerar na fase de pré-aquisição são os seguintes:

- Soluções a residirem em infraestrutura própria da CMA:
    - Apresentação de relatório com resultado positivo de análise a vulnerabilidades;
    - Toda a informação confidencial de clientes que circule na internet deve ser cifrada com SSL/TLS e com chaves de 256 bits, no mínimo;
    - A aplicação deve suportar federação de identidades SAML v2;
    - Sempre que possível o fornecedor deve apresentar evidências de testes de penetração recentes efetuados por uma terceira parte.

- Soluções a residirem em infraestrutura externa:
    - Apresentação de relatório com resultado positivo de análise a vulnerabilidades;
    - Toda a informação confidencial de clientes que circule na internet deve ser cifrada com SSL/TLS e com chaves de 256 bits, no mínimo;
    - A aplicação tem que suportar federação de identidades SAML v2;
    - Sempre que possível o fornecedor deve permitir uma auditoria de segurança às instalações onde a aplicação ficará alojada. Em alternativa, pode ser apresentado um relatório recente de auditoria (s) de segurança, realizadas a esse ambiente;
    - Sempre que possível, o fornecedor deve:
        - Apresentar evidências de testes de penetração recentes efetuados por uma terceira parte;
        - Autorizar a CMA a executar testes de penetração ao ambiente, a serem concretizados por esta ou por uma terceira parte.

Os requisitos de arquitetura de novos sistemas são:

- Toda a informação confidencial de cliente que transite na internet deve estar cifrada, recorrendo SSL ou TLS com chaves mínimas de 256 bits;
- Sempre que possível a arquitetura da solução deve consistir em três camadas distintas ao nível de hardware e aplicações:
    - Servidores web;
    - Servidores aplicacionais;
    - Servidores de base de dados;

- Os servidores web devem ser localizados numa zona DMZ e os restantes servidores (aplicacionais e base de dados) em zonas próprias e distintas;
- Os servidores de base de dados não devem residir em zona DMZ;
- Devem ser utilizados mecanismos seguros para transferência maciça de dados com informação confidencial de clientes, utilizando-se sFTP ou HTTPs.
- Devem ser evitados file shares de Windows que atravessem zonas de rede. Quando não exista a possibilidade de os evitar, todos os FileShares devem ser protegidos adequadamente por regras de firewall sendo somente permitido tráfego para e de endereços de IP específicos;
- Qualquer aplicação deve ser arquitetada como se estivesse exposta à internet.

Os requisitos para a autenticação de utilizadores são:

- Os sistemas devem forçar a federação de identidades via AD / SAML v2;
- Os sistemas que não permitam a federação de identidades via AD devem forçar a implementação da política de passwords em vigor;

- A federação de identidades em entidades fora do domínio CMA não deve ser utilizada, exceto se a informação for considerada pública;
- A informação de suporte ao processo de autenticação deve sempre utilizar um canal seguro para transmissão, independentemente se esta atravessa a internet ou não.

Os requisitos para autorização de utilizadores são:

- A autorização de acesso de utilizadores deve ser controlada via ACL's e deve ser implementada via grupos de segurança, regras de acesso em tabelas SQL ou controlos de autorização implementados nativamente nas aplicações;
- As decisões de autorização nos sistemas devem ser baseadas nos privilégios concedidos ao grupo ou função assignado à conta de utilizador.

Os requisitos para cifra e integridade dos dados são:

- Toda a informação não pública que circule na rede deve ser sujeita a cifra mediante a utilização de canais HTTPS (SSL/TLS);
- Cifras simétricas com chaves menores do que 128 bits ou assimétricas com menos de 2056 bits não devem ser utilizadas por qualquer servidor web;
- O SSL v2 não deve ser suportado em qualquer servidor web;
- A cifra de informação deve ser sempre baseada em metodologias e algoritmos standard, sempre pré-aprovadas pela CMA;
- Sempre que possível a informação residente em base de dados deve ser cifrada.

Os requisitos para logs de auditoria e monitorização são:

- Os sistemas devem evitar registar informação sensível nos ficheiros de log;
- Os sistemas devem implementar o princípio de "menor privilégio", ou seja, os sistemas, aplicações e funcionalidades devem ter somente privilégios de escrita no ficheiro de log e os privilégios de leitura devem ser restritos a utilizadores ou processos específicos pré-identificados e autorizados;
- Sempre que possível os registos de log devem ser enviados para um repositório separado, central, para assegurar a disponibilidade e integridade da informação caso o sistema seja comprometido.

4. Política para aceitação de sistemas

A aceitação de novos sistemas de informação, atualizações ou novas versões aplicáveis a sistemas de informação registados no inventário de ativos da CMA requer:

- Seja evidenciada a execução das fases específicas de verificação do estado de conformidade com os requisitos de controlos de segurança da informação, quando na execução interna de projeto de desenvolvimento ou melhoria de sistemas;
- Seja efetuada uma validação de uma resposta eficaz aos requisitos de segurança da informação formalizados na fase de aquisição ou desenho de novos sistemas ou de melhoria a sistemas existentes;

As principais técnicas aceites para validação de requisitos de segurança da informação são:

- Diagnósticos de vulnerabilidade de segurança;
- Testes de penetração;
- Análise ao código fonte;
- Revisão de código ou ambiente por terceiros autorizados.

Em caso de validação negativa de resposta aos requisitos de segurança formalizados, o ambiente (novo ou modificado) não poderá transitar para ambiente produtivo.

5. Procedimentos para controlo de alterações a sistemas

Cumulativamente ao estabelecido na Política de Gestão de Alterações do SGSI, com a finalidade de controlar as alterações com impacto significativo a sistemas de informação da CMA, os seguintes passos devem ser incorporados na estruturação de processos de gestão de alterações, respeitando a presente ordem de apresentação:

- Avaliação da autoridade do solicitante para solicitar a alteração;
- Identificação de todo o software, informação, bases de dados e hardware que necessitarão de alterações;
- Análise à continuidade após a implementação da alteração do cumprimento de requisitos de arquitetura, controlo de acessos, criptografia, salvaguarda da informação e outros identificados como relevantes;
- Obtenção de aprovação das propostas de alterações globais pelos responsáveis dos diversos ativos implicados, antes do início dos trabalhos de alteração;
- Atualização de documentação de suporte ao sistema e de alterações a controlos de segurança.

Sempre que possível devem ser mantidos registos apropriados da execução dos diferentes passos acima identificados.

6. Validade e gestão de documentos

Este documento é válido a partir de 15/04/2021.

O responsável deste documento é o Gestor da Segurança da Informação, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

Tipo de documento:	**Política**		
Criado por:	Divisão de Sistemas e Tecnologias de Informação e Comunicação		
Aprovado por:	Comissão da Segurança da Informação		
Nível de confidencialidade	**Público**		
Data:	**Versão/Revisão**	**Criado/Modificado por:**	**Descrição da alteração:**
31-07-2020	00/00	Anabela Lourenço, Ricardo Jorge Simões e Ricardo Madeira Simões	Esboço básico do documento
07-08-2020	01/00	Anabela Lourenço, Ricardo Jorge Simões e Ricardo Madeira Simões	Conclusão do documento *Nota: Separação do Manual do SGSI*
26-10-2021	01/01	Anabela Lourenço, Cidália Jorge, Ricardo Jorge Simões e Ricardo Madeira Simões	Atualização do ficheiro. Erros detetados cabeçalho. Publicação na Intranet
15/11/2023	01/02	Cidália Jorge/ Ricardo Jorge Simões	Revisão do texto e novo cabeçalho e histórico de versões
14/10/2024	01/03	Cidália Jorge/ Ricardo Jorge Simões	Revisão do texto
29/11/2024	01/04	Cidália Jorge/ Ricardo Jorge Simões	Política atualizada e adequada à versão da norma ISO27001:2022
27/05/2025	01/05	Cidália Jorge/ Ricardo Jorge Simões	Revisão do texto

Índice

1. Finalidade, âmbito e utilizadores

O objetivo desta Política de alto nível é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação.

Esta política aplica-se a todo o Sistema de Gestão da Segurança da Informação (SGSI), como definido no Manual do SGSI.

Os utilizadores deste documento são trabalhadores e colaboradores da Câmara Municipal da Amadora (CMA), assim como as partes externas relevantes.

O proprietário do documento é a Comissão de Segurança da Informação, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de trabalhadores, colaboradores e terceiros que têm um papel no SGSI, mas não conhecem este documento
- não conformidade do SGSI com as leis e as regulamentações, as obrigações contratuais e outros documentos internos da organização
- ineficácia da manutenção e da implementação do SGSI
- responsabilidades confusas na implementação do SGSI

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas 5.2, 5.3, 6.2, 7.4 e A.6.3
- Manual do SGSI
- Metodologia de avaliação e tratamento de riscos
- Declaração de aplicabilidade
- Lista de obrigações legais, regulamentares e outras
- PT10 - Procedimento de gestão de incidentes

3. Terminologia básica de segurança da informação

Confidencialidade – características das informações que estão disponíveis somente para pessoas autorizadas ou sistemas.

Integridade - características das informações que são alteradas somente por pessoas autorizadas.

Disponibilidade - características das informações que somente podem ser acedidas por pessoas autorizadas, quando for necessário.

Segurança da informação - preservação da confidencialidade, integridade e disponibilidade da informação

Manual do Sistema de gestão da segurança da informação - a parte do sistema de gestão que cuida do planeamento, implementação, manutenção, revisão e melhoramento da segurança da informação.

4. Gestão da segurança da informação

4.1 Objetivos e medição

Os objetivos gerais para a gestão de segurança da informação são os seguintes: criar uma melhor imagem no município e no país, reduzir os danos causados por possíveis incidentes, e, se eles estão em linha com os objetivos de negócios da organização, estratégia e plano de negócios. O Responsável de Segurança da Informação é responsável por rever estes objetivos SGSI gerais e por definir novos objetivos. Os objetivos dos controlos de segurança ou grupos de controlos são definidos pela Comissão de Segurança da Informação (CSI), e aprovados pela Comissão de Segurança da Informação (CSI) na Declaração de aplicabilidade. Todos os objetivos devem ser revistos pelo menos uma vez por ano.

A Comissão de Segurança da Informação é responsável por definir o método para a medição da realização dos objetivos – a medição será executada pelo menos uma vez por ano e o Gestor do Processo irá analisar a avaliar os resultados da medição e reportá-los para a Gestão de Topo como material para a revisão pela gestão e análise crítica.

O Responsável de Segurança da Informação é responsável por registar os detalhes sobre os métodos de medição, periodicidades e resultados no Relatório de medição (Programa anual de gestão).

Os pontos cruciais para a Gestão da Segurança da Informação são:

- Abordagem para o estabelecimento de objetivos;
- Princípios orientadores para a Segurança da informação;
- Princípios de ação relacionados com a Segurança da Informação;
- Abordagem por processos;
- Abordagem para a melhoria contínua do Sistema;
- Abordagem para a gestão da conformidade legal, regulatória e contratual.

4.2 Requisitos de segurança da informação

Esta Política e todo o SGSI deve estar em conformidade com os requisitos legais e regulamentares da organização na área de segurança da informação, bem como com as obrigações contratuais.

Lista detalhada de todos os requisitos contratuais e legais na Lista de obrigações regulamentares, contratuais e outras.

4.3 Controlos da segurança da informação

Os processos para selecionar os controlos estão definidos na Metodologia de avaliação e tratamento de riscos.

Os controlos selecionados e sua condição de implementação estão descritos na Declaração de Aplicabilidade.

4.4 Responsabilidades

As responsabilidades básicas para o SGSI são:

- A Gestão de Topo é responsável por garantir que o SGSI seja implementado de acordo com esta Política e para garantir todos os recursos necessários;
- A Comissão de Segurança da Informação é responsável pela coordenação operacional do SGSI, bem como reportar sobre o desempenho do SGSI;

- O Responsável da Segurança da Informação (RSI) deve analisar o SGSI pelo menos uma vez por ano ou sempre que ocorrer uma mudança importante e elaborar minutas sobre a reunião. A finalidade da revisão da gestão é definir a adequabilidade e a eficácia do SGSI;
- A CSI implementará programas de sensibilização e treino sobre segurança da informação para os trabalhadores e colaboradores;
- A proteção da integridade, disponibilidade e confidencialidade é responsabilidade do proprietário de cada ativo;
- Todos os incidentes e as fragilidades de segurança devem ser reportados, ao serviço de informática, ao Responsável de Segurança da Informação e, por sua vez, este informa a Gestão de Topo;
- O RSI irá definir quais as informações, relativas à segurança da informação, serão comunicadas, às partes interessadas, por quem e quando;
- A CSI é responsável por adotar e implementar um Plano de treino e consciencialização, que se aplique a todas as pessoas que têm uma função na gestão da segurança da informação.

4.5 Comunicação da política

A Gestão de Topo deve garantir que todos trabalhadores e colaboradores da CMA, bem como todos as partes externas interessadas conheçam esta Política.

5. Suporte para a implementação do SGSI

A Gestão de Topo declara que a implementação do SGSI e seu contínuo melhoramento serão suportadas pelos recursos apropriados para alcançar todos os objetivos definidos nesta Política, assim como considerar todos os requisitos identificados.

Amadora, 27 de maio de 2025

O Vereador do Pelouro,

Ana Venâncio

Assinado por: **ANA CARLA DE CARVALHO VENÂNCIO**
Num. de Identificação: 10536757
Data: 2025.07.21 19:51:44+01'00'

____

POLÍTICA DE SEGURANÇA DO FORNECEDOR

Tipo de documento:	**Política**		
Criado por:	Divisão de Sistemas e Tecnologias de Informação e Comunicação		
Aprovado por:	Comissão da Segurança da Informação		
Nível de confidencialidade	**Público**		
Data:	**Versão/Revisão**	**Criado/Modificado por:**	**Descrição da alteração:**
05/12/2023	01/00	Cidália Jorge, Ricardo Jorge Simões	Revisão do texto
15/10/2024	02/01	Cidália Jorge, Ricardo Jorge Simões	Novo template. Revisão do texto, novo cabeçalho e histórico de versões

Índice

1. Finalidade, âmbito e utilizadores

Com a finalidade de mitigar os riscos associados a acessos a ativos de informação e definir as regras para o relacionamento de suporte de fornecedores da Câmara Municipal da Amadora, é imperativo que sejam delineados, comunicados e formalmente acordados com estes, os controlos de segurança apropriados à proteção da informação, incluindo prestadores de serviços em nuvem.

Este documento é aplicável a todos fornecedores e parceiros que têm a capacidade de influenciar a confidencialidade, integridade e disponibilidade de informações sensíveis da Câmara Municipal da Amadora.

Os utilizadores deste documento são a CSICMA e a Divisão de Aprovisionamento responsáveis pela relação com fornecedores e parceiros da Câmara Municipal da Amadora.

O proprietário do documento é o Responsável de Segurança da Informação, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade e significância de incidentes resultantes de atividades de fornecedores e parceiros
- quantidade de contratos onde o proprietário do contrato não está definido

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.7, A.5.11, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.6.1, A.6.2, A.6.3 e A.8.30
- Metodologia de avaliação e tratamento de riscos
- Relatório de avaliação e tratamento de risco
- Política de Controlo de Acessos
- Declaração de Confidencialidade

3. Relação com fornecedores e parceiros

A proteção da informação crítica sob responsabilidade da Câmara Municipal da Amadora é um requisito para o estabelecimento de contratos com fornecedores que a ela tenham necessidade de aceder.

Face ao acima exposto, deliberou a Câmara Municipal da Amadora a implementação de um Sistema de Gestão da Segurança da Informação para proteção de informação crítica sob sua responsabilidade.

Ao abrigo da presente política a informação alvo de proteção, doravante denominada por "Informação Crítica", centra-se, mas não se restringe, a:

- Quaisquer dados ou conhecimentos que requerem que a sua utilização seja restrita a elementos pré-autorizados e que em caso de incidente de segurança, possa causar impactos substanciais na imagem, reputação ou confiança da CMA
- Informação que contenha:
  - Dados Pessoais;
  - Dados de Saúde;
  - Dados sobre Meios de Pagamento ou suas transações;
  - Dados sobre Propriedade Intelectual.
- Informação que esteja sujeita a medidas de proteção especial devido a requisitos legais ou contratuais;
- Outros dados ou conhecimentos, não públicos ou confidenciais, de suporte às atividades da Câmara Municipal da Amadora.

Assim, a qualquer fornecedor da CMA que necessite de aceder a informação crítica da CMA é requerido:

- O conhecimento antecipado e aderência total ao expresso na presente política;

- A assinatura formal, por quem represente a entidade, de um "Acordo de confidencialidade e não divulgação de informação" que reverte, no todo ou em parte, os requisitos estabelecidos na presente política;
- Que ponha em prática as medidas técnicas e organizativas adequadas para proteger dados pessoais e outra informação crítica da CMA contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito;
- Que, declara e garanta, enquanto subcontratado, que o tratamento de dados pessoais é efetuado em conformidade com o Regulamento Geral de Proteção de Dados ("RGPD"), nomeadamente, sem limitar, em conformidade com os direitos, liberdades fundamentais e dignidade das pessoas singulares e coletivas, com particular referência à privacidade e ao direito à proteção de dados pessoais

- Que implemente mecanismos de controlo que assegurem:
  - Impedir o acesso de pessoa não autorizada às suas instalações utilizadas para o tratamento de informação crítica da CMA (controlo da entrada nas instalações);
  - Impedir que suportes de dados, que contenham informação crítica da CMA, possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados);
  - Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados (controlo da inserção) de informação crítica da CMA;
  - Impedir que sistemas de tratamento automatizados de dados, inerentes à Informação crítica da CMA, possam ser utilizados por pessoas não autorizadas (controlo da utilização);
  - Garantir que as pessoas autorizadas só possam ter acesso aos dados, inerentes à Informação crítica da CMA, abrangidos por autorização previamente concedida (controlo de acesso);
  - Garantir antecipadamente a verificação das entidades autorizadas pela CMA a quem possam ser transmitidos dados inerentes à Informação crítica da CMA através de mecanismos de transmissão eletrónica de dados (controlo da transmissão);
  - Garantir que se possa verificar, à posteriori, em prazo adequado à natureza do tratamento, quais os dados inerentes à Informação crítica que tenham sido introduzidos, quando e por quem (controlo da introdução);
  - Impedir que, na transmissão de dados, inerentes à Informação crítica da CMA, bem como no transporte de seus suportes, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).

É aceite o tratamento, pelo fornecedor, da informação crítica exclusivamente para efeitos do objeto da contratação formalizada. Qualquer utilização que extravase este é absolutamente proibida, salvo consentimento formalizado pela Câmara Municipal da Amadora.

O fornecedor está autorizado a:

- Aceder, no todo, ou em parte, à informação referida;
- Alterar, no todo ou em parte, a informação referida, corrigindo-a em total conformidade quando solicitado pelo detentor fidedigno dos dados em causa.

O fornecedor não está autorizado a:

- Transmitir, no todo ou em parte, a informação referida para outrem sem autorização antecipada e formalmente expressa pela Câmara Municipal da Amadora;
- Eliminar, no todo ou em parte, a informação referida.

O fornecedor está obrigado a conhecer, cumprir e fazer cumprir a Política de Segurança da Informação em vigor na Câmara Municipal da Amadora, por ser relevante para o correto cumprimento do objeto do contrato, nomeadamente:

- A Política de Segurança da Informação da Câmara Municipal da Amadora;
- A Política de Segurança do Fornecedor;

Quando, em face a uma situação potencial ou situação factual de ocorrência de um incidente de segurança da informação (i.e., um incidente que possa colocar em causa a integridade, a confidencialidade e/ou a disponibilidade da informação crítica da Câmara Municipal da Amadora, o fornecedor está obrigado a cumprir escrupulosamente os Procedimentos de Resposta a Incidentes de Segurança da Informação que estejam em vigor à data e cujo conteúdo necessário será dado a

conhecer na reunião de arranque da implementação do serviço adjudicado e/ou da entrega e configuração do equipamento adjudicado.

É obrigação do fornecedor:

- Ministrar ações de sensibilização ou formação a todos os elementos sob sua responsabilidade e integrados nos serviços contratados, com o limite mínimo de oito horas anuais, sobre as Políticas da Segurança da Informação acima referidas;
- Ministrar uma ação de sensibilização ou formação, com o limite mínimo de duas horas, a qualquer novo elemento sob sua responsabilidade que seja autorizado a aceder à informação referida e antes de este aceder a esta.

É expressamente proibido ao fornecedor a subcontratação de qualquer entidade, que para o desempenho das suas atividades necessite de acesso a informação crítica da Câmara Municipal da Amadora, sem autorização formal expressa e antecipada desta.

A mera solicitação formal para acesso à referida informação não pressupõe posterior autorização da Câmara Municipal da Amadora.

Em caso de autorização emanada pela Câmara Municipal da Amadora, esta possuirá, devidamente referenciados, os controlos da segurança da informação e as suas boas práticas, para os quais será requerida conformidade pela parte contratada e sua subcontratada.

A gestão de acessos a ativos de informação e a ativos de suporte a esta, sejam estes locais ou meios em que estes residam, redes ou serviços, inerentes à execução de serviços contratados a fornecedores da Câmara Municipal da Amadora, segue impreterivelmente o estabelecido no documento Políticas da Segurança da Informação da Câmara Municipal da Amadora - Política de Controlo de Acessos desta última entidade.

É concedido à Câmara Municipal da Amadora o direito de auditar, sempre que esta entenda necessário, os processos e controlos da segurança da informação do fornecedor, no âmbito da informação crítica da CMA, a fim de se verificar a conformidade destes para com os objetivos e requisitos de proteção dessa informação.

Qualquer situação de não conformidade do fornecedor para com os requisitos de proteção da informação crítica da Câmara Municipal da Amadora, será alvo de registo, pelas partes, com atribuição de um identificador único e posterior resolução, a custos do fornecedor, de acordo com resoluções e calendário expresso formalmente pela CMA.

Em caso de litígio legal, o foro a utilizar é o da Comarca da Amadora com expressa renúncia a qualquer outro.

Constitui obrigação do fornecedor a apresentação anual, à Câmara Municipal da Amadora, de relatório independente sobre a eficácia dos controlos de segurança por ela implementados face aos requisitos de proteção da informação ora expressos. Caso se identifique qualquer situação de não conformidade, aplica-se o expresso no parágrafo anterior.

Constitui obrigação do fornecedor o cumprimento objetivo dos requisitos de segurança ora expressos. Em caso de incumprimento, será aplicada uma sanção que poderá originar, no limite, a cessação da prestação dos serviços objeto do presente contrato e, cumulativamente, uma sanção pecuniária a determinar.

Os produtos ou serviços a adquirir ou a utilizar pelo fornecedor no contexto do contrato estabelecido deverão obrigatoriamente contemplar controlos adequados de segurança da informação que permitam assegurar os níveis de confidencialidade, disponibilidade e integridade requeridos para proteção da informação crítica da CMA.

Neste contexto, salientam-se entre outros, os seguintes objetivos de controlo base que o fornecedor terá de alcançar:

- Assegurar a proteção da informação em cenários de teletrabalho e na utilização de dispositivos móveis;

- Assegurar que os seus colaboradores e seus prestadores de serviço compreendem as suas responsabilidades, e que são adequados para as funções para as quais estão a ser considerados;
- Assegurar que os seus colaboradores e seus prestadores de serviço estão conscientes e cumprem as suas responsabilidades no contexto da segurança da informação da CMA;
- Proteger os interesses da CMA no processo de cessação ou alteração da relação contratual com seus colaboradores ou seus prestadores de serviço;
- Identificar os seus ativos utilizados no contexto do fornecimento e definir responsabilidades de proteção apropriadas;
- Assegurar que a informação crítica da CMA recebe um nível adequado de proteção, de acordo com a sua importância para esta;
- Prevenir a divulgação não autorizada, modificação, remoção ou eliminação da informação crítica da CMA armazenada em suportes de dados;
- Limitar o acesso à informação crítica da CMA e aos seus recursos de processamento dessa informação;
- Assegurar o acesso de utilizadores autorizados e prevenir o acesso não autorizado a sistemas e serviços de suporte à informação crítica da CMA;
- Tornar os utilizadores responsáveis pela proteção da sua informação de autenticação;
- Prevenir o acesso não autorizado a sistemas e aplicações de suporte à informação crítica da CMA;
- Assegurar a utilização adequada e eficaz de criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação crítica da CMA;
- Prevenir o acesso físico não autorizado, os danos e as interferências na informação e nos recursos de processamento de informação de suporte à informação crítica da CMA;
- Prevenir a perda, dano, furto ou comprometimento de ativos e interrupção das operações de suporte à informação crítica da CMA;
- Assegurar a operação correta e segura dos recursos de processamento de informação de suporte à informação crítica da CMA;
- Assegurar que a informação e os recursos de processamento de informação crítica da CMA estão protegidos contra código malicioso;
- Proteger contra a perda de dados da informação crítica da CMA;
- Registar eventos e gerar evidências, daqueles que estejam relacionados com atividades dos utilizadores, exceções, falhas e eventos de segurança da informação crítica da CMA;
- Assegurar a integridade dos sistemas de produção de suporte à informação crítica da CMA;
- Prevenir a exploração de vulnerabilidades técnicas dos sistemas de suporte à informação crítica da CMA;
- Assegurar a proteção da informação à informação crítica da CMA nas redes e nos seus recursos de processamento de informação;
- Manter a segurança da informação à informação crítica da CMA que seja transferida dentro da organização e para qualquer entidade externa;
- Assegurar que a segurança da informação à informação crítica da CMA é uma parte integrante dos sistemas de informações ao longo do todo o seu ciclo de vida;
- Assegurar que a segurança da informação à informação crítica da CMA é concebida e implementada no âmbito do ciclo de vida do desenvolvimento de sistemas de informação;
- Assegurar a proteção dos dados de suporte à informação crítica da CMA usados para testes;
- Assegurar a proteção dos ativos de suporte à informação crítica da CMA que estão acessíveis aos seus fornecedores;
- Manter o nível acordado de segurança da informação e de disponibilização de serviços contratados aos seus fornecedores, alinhado com a presente política;
- Assegurar uma abordagem consistente e eficaz à gestão de incidentes de segurança da informação, no contexto do fornecimento, incluindo a comunicação de eventos e pontos fracos de segurança;
- Assegurar a continuidade da segurança da informação à informação crítica da CMA nos modelos, planos e sistemas de gestão da continuidade do seu negócio;
- Assegurar a disponibilidade dos recursos de processamento da informação à informação crítica da CMA;
- Evitar violações de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas com a segurança da informação crítica da CMA e de quaisquer dos seus requisitos de segurança;
- Assegurar que a segurança da informação crítica da CMA é implementada e operada de acordo com políticas e procedimentos aprovados pela Câmara Municipal da Amadora;

Caso o fornecedor necessite de recorrer a subcontratação de terceiros (pessoas ou empresas) para prestação dos serviços de tecnologias de informação e comunicação, compromete-se a:

- Dar conhecimento e obter consentimento formal da Câmara Municipal da Amadora;
- Acordar com a entidade subcontratada a obrigatoriedade de cumprimento dos requisitos expressos na presente política;
- Acordar com a entidade subcontratada a necessidade de cumprir com os requisitos de segurança subjacentes ao serviço contratualizado.

Caso o fornecedor necessite de integrar componentes de terceiros (pessoas ou empresas) nos produtos a fornecer, deverá:

- Dar conhecimento e obter consentimento formal da Câmara Municipal da Amadora;
- Validar o cumprimento dos requisitos de segurança desses componentes, em acordo com os requisitos de segurança da informação da Câmara Municipal da Amadora.

É obrigação do fornecedor, definir e implementar um processo e procedimentos de monitorização e validação dos requisitos de segurança estabelecidos, devendo ainda reportar não-conformidades ou incidentes de segurança, de acordo com a Política e Procedimentos de Resposta a Incidentes de Segurança da Informação estabelecidos pela Câmara Municipal da Amadora.

É obrigação do fornecedor, identificar os produtos ou serviços críticos que possam ter impacto na manutenção do serviço contratado, através:

- Da constituição de um inventário dos produtos e serviços críticos para com os objetivos do serviço contratado;
- Da atualização anual desse inventário, ou sempre que existir uma alteração que obrigue a sua revisão;
- Da identificação, definição, desenvolvimento, aplicação e teste de planos de contingência, com vista à manutenção da funcionalidade dos produtos ou serviços críticos inventariados.

O fornecedor deve implementar nos seus processos, os procedimentos conducentes à inclusão e atualização, no inventário dos produtos e serviços críticos, de informação de rastreamento da cadeia de fornecimento dos componentes críticos que os compõem.

É obrigação do fornecedor, implementar um processo de garantia de qualidade (Quality Assurance), que assegure o funcionamento correto e sem falhas dos produtos fornecidos à Câmara Municipal da Amadora, devendo disponibilizar a ficha técnica do produto e informação dos resultados dos testes de qualidade realizados.

É obrigação do fornecedor, acomodar e promover as regras emanadas pela Câmara Municipal da Amadora para partilha de informações com a sua cadeia de fornecimento subcontratada a fim de que seja assegurado o funcionamento correto e sem falhas dos produtos ou serviços fornecidos a esta, assegurando sempre a segurança da informação de suporte ao objeto do contrato. Potenciais questões sobre requisitos ou compromissos para partilha de informação devem ser dirigidos por escrito diretamente à Câmara Municipal da Amadora.

É obrigação do fornecedor, gerir os riscos associados à disponibilidade e fornecimento dos produtos e serviços contratados, nomeadamente de cada um dos seus componentes, devendo, sempre que possível, reduzir esses riscos a um nível aceitável e controlável.

A informação dos riscos identificados, sua análise e opções de mitigação devem ser disponibilizadas à Câmara Municipal da Amadora, sempre que solicitadas.

A Câmara Municipal da Amadora efetuará, de forma regular, atividades de monitorização, revisão e auditoria aos serviços disponibilizados pelos seus fornecedores. A sua realização contemplará:

a) A monitorização dos níveis de desempenho de serviço, verificando o cumprimento dos acordos;
b) A revisão dos relatórios de serviço produzidos pelo fornecedor;
c) A análise conjunta de relatórios de auditores independentes, quando existirem, e seguimento das ocorrências aí identificadas;

d) A análise de incidentes de segurança da informação reportados, ou não, pelo fornecedor;
e) A revisão de logs de auditoria e registos de eventos de segurança da informação, problemas operacionais, falhas, deteção de falhas e interrupções de serviço do fornecedor, relacionadas com a prestação dos serviços contratados;
f) A revisão e resolução de questões de segurança da informação do fornecedor para com os seus próprios fornecedores;
g) A avaliação de que o fornecedor mantém a capacidade de serviço suficiente, bem como planos de continuidade viáveis, no sentido de garantir que são mantidos os níveis de serviço adequados no caso de acidente ou catástrofe.

As alterações ao fornecimento dos serviços pelos fornecedores, incluindo a manutenção e melhoria das suas políticas de segurança da informação e dos procedimentos e controlos existentes, serão geridas tendo em consideração a criticidade da informação, dos sistemas e processos envolvidos na prestação dos serviços contratados.

O presente documento rege-se pela Lei Portuguesa.

As questões que se suscitarem sobre a interpretação, execução ou aplicação das regras constante do Regulamento e que não sejam solucionadas por acordo entre as partes serão dirimidas pelo Tribunal da Comarca da Amadora, com expressa renúncia a qualquer outro.

Qualquer dúvida ou esclarecimento adicional necessário relacionado com a segurança da Informação da Câmara Municipal da Amadora ou com políticas ou procedimentos em vigor nesta matéria deverá ser endereçado para: geral@cm-amadora.pt.

AMADORA
Câmara Municipal
Departamento de Modernização e Tecnologias da Informação e Comunicação . DMTIC
Divisão de Sistemas e Tecnologias de Informação e Comunicação. DSTIC

DECLARAÇÃO DE CONFIDENCIALIDADE PARA EMPRESAS PRESTADORAS DE SERVIÇOS

A Empresa "………………………..com sede em ……..………….., Pessoa Coletiva n.º…………………., representada por ……………..……., na qualidade de……….………….., declara comprometer-se a cumprir os pontos abaixo descritos, referentes à confidencialidade da informação no âmbito dos serviços que vai prestar à Câmara Municipal da Amadora;

- Garantir a confidencialidade e proteção da informação identificada como protegida, confidencial ou com outra expressão de igual significado, revelada pela Câmara Municipal da Amadora, com a exclusiva finalidade de dar cumprimento ao contrato de prestação de serviços celebrado;
- **Garante e declara, enquanto subcontratado, que o tratamento de dados pessoais é efetuado em conformidade com o Regulamento Geral de Proteção de Dados ("RGPD"), nomeadamente, sem limitar, em conformidade com os direitos, liberdades fundamentais e dignidade das pessoas singulares e coletivas, com particular referência à privacidade e ao direito à proteção de dados pessoais**
- Comprometer-se a cumprir os requisitos constantes da documentação enviada, nomeadamente Política de Segurança da Informação e Política de Segurança do Fornecedor;
- Esta declaração obriga igualmente todos os colaboradores da empresa prestadora do serviço, em função permanente ou temporária;
- Compromete-se igualmente a restringir a divulgação das informações confidenciais unicamente a quem essas informações sejam essenciais para o desenvolvimento do projeto ou adjudicação em causa;
- A obrigação de confidencialidade vigorará após a cessação, seja por que motivo for, da colaboração do Declarante na Câmara Municipal da Amadora.

Amadora, ….

____

Representante da Empresa (cargo)

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt