



CÂMARA MUNICIPAL DE PENALVA DO CASTELO

Processo n.º39/2022 GF

AJUSTE DIRETO

Serviço de segurança e resposta a incidentes

(Ao abrigo da alínea d), n.º 1 do artigo 20.º do Código dos Contratos Públicos aprovado pelo decreto-lei n.º 18/2008, de 29 de janeiro, doravante designado por CCP)

CADERNO DE ENCARGOS
(Artigo 42.º do CCP)

PARTE I – CLÁUSULAS JURIDICAS

Capítulo I

Disposições gerais

Cláusula 1.^a

Objecto

O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto principal o “serviço de segurança e resposta a incidentes”.

Cláusula 2.^a

Local da prestação do serviço

O local da prestação do serviço situa-se no edifício dos Paços do Concelho.

Cláusula 3.^a

Contrato

1 – O contrato é composto pelo respectivo clausulado e os seus anexos.

2 - O contrato a celebrar integra ainda os seguintes elementos:

- a) Os suprimentos dos erros e omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
- b) Os esclarecimentos e as rectificações relativos ao Caderno de Encargos;
- c) O presente Caderno de Encargos;
- d) A proposta adjudicada;
- e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3 - Em caso de divergência entre os documentos referidos no número anterior, a prevalência é determinada pela ordem pela qual aí são indicadas.

4 – Em caso de divergência entre os documentos referidos no nº2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99º do Código dos Contratos Públicos e aceites pelo adjudicatário, nos termos do disposto no artigo 101º desse mesmo diploma legal.

Cláusula 4.^a

Prazo de vigência do contrato

1 - O contrato a celebrar, em conformidade com os respetivos termos e condições e o disposto na lei sem prejuízo das obrigações que devam perdurar para além da cessação do contrato, tem em conta os seguintes prazos:

- a) O serviço a realizar no âmbito da presente consulta, deverá ser executado no período de 12 meses, tendo início no dia 01 de janeiro de 2023

Capítulo II

Obrigações contratuais

Secção I

Obrigações do prestador de serviços

Subsecção I

Disposições gerais

Cláusula 5.^a

Obrigações principais do prestador de serviços

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente caderno de encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o prestador de serviços as seguintes obrigações principais:

a) Obrigação de realizar a prestação do serviço com zelo, diligência e boa colaboração, sob pena de responder perante eventuais danos.

2. A título acessório, o prestador de serviços fica ainda obrigado, designadamente, a recorrer aos meios humanos, materiais e informáticos que sejam necessários e adequados à prestação do serviço, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo, sem qualquer encargo para as entidades adjudicantes.

Cláusula 6.^a

Conformidade e garantia técnica

O prestador dos serviços fica sujeito, com as devidas adaptações e no que se refere aos elementos entregues à Câmara Municipal de Penalva do Castelo em execução do contrato, às exigências técnicas legalmente estipuladas, obrigações do fornecedor e prazos respectivos aplicáveis aos contratos de aquisição de bens móveis, nos termos do Código dos Contratos Públicos e demais legislação aplicável.

Subsecção II

Dever de sigilo

Cláusula 7.^a

Objeto do dever de sigilo

1 – O prestador de serviços deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à Câmara Municipal de Penalva do Castelo, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.

2 – A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objecto de qualquer uso ou modo de aproveitamento que não o destinado directa e exclusivamente à execução do contrato.

3 – Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respectiva obtenção pelo fornecedor ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou entidades administrativas competentes.

Cláusula 8.^a

Prazo do dever do sigilo

O dever de sigilo mantém-se em vigor até ao termo de dois anos a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à protecção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas colectivas.

Secção II

Obrigações do contraente público

Cláusula 9.^a

Preço contratual

1 - Pela prestação dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a Câmara Municipal de Penalva do Castelo deve pagar ao adjudicatário o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.

2 – O preço referido no número anterior não pode, em qualquer caso, ser superior a 9 000,00€ (nove mil euros) acrescido do IVA, e inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, incluindo as despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte e armazenamento e manutenção de meios materiais,

Cláusula 10.^a

Condições de pagamento

1 – As quantias devidas pela Câmara Municipal de Penalva do Castelo, nos termos da cláusula anterior, devem ser pagas no prazo proposto pelo prestador do serviço, não podendo ser inferior a trinta dias após a recepção pela Câmara Municipal de Penalva do Castelo das respectivas facturas, as quais só podem ser emitidas após o vencimento da obrigação respectiva.

2 – Para os efeitos do número anterior, a obrigação considera-se vencida com a entrega dos elementos a desenvolver pelo prestador de serviços ao abrigo do contrato.

3 – Em caso de discordância por parte da Câmara Municipal de Penalva do Castelo, quanto aos valores indicados nas facturas, deve esta comunicar ao prestador de serviços, por escrito, os respectivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou proceder à emissão de novas facturas corrigidas.

4 – Desde que devidamente emitidas e observado o disposto no nº1, as facturas são pagas através de cheque ou de transferência bancária.

Cláusula 11.^a

Proteção de dados

1. O contrato, no que respeita ao tratamento de dados pessoais, tem a justificação legal do tratamento de dados pessoais necessários e fundamentais à prossecução da missão, atribuições e competências do Município de Penalva do Castelo;

2. Para efeitos do disposto no número anterior, a entidade adjudicante e a entidade adjudicatária estão sujeitas ao cumprimento do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados), adiante designado RGPD, sendo o Município de Penalva do Castelo responsável pelo tratamento de dados e a entidade adjudicatária o subcontratante, na aceção do n.ºs 7 e 8 do artigo 4.º, do n.º 1 do artigo 24.º e do n.º 1 do artigo 28.º todos do RGPD.

3. O tipo de dados, as categorias dos titulares dos dados, as operações de tratamento de dados pessoais bem como as condições de conservação e armazenamento e respetivo prazo de conservação serão devidamente especificados em anexo ao presente contrato, quando assim se justifique.

4. Entre as partes contratantes, respetivamente enquanto responsável pelo tratamento de dados e subcontratante, são estabelecidos e reciprocamente aceites os seguintes direitos e obrigações:

a) O Município de Penalva do Castelo (*entidade adjudicatária*) comunica o contacto telefónico e o endereço de correio eletrónico do seu Data Protection Officer (Encarregado de Proteção de Dados, DPO):

DPO: Anselmo Gomes de Almeida Sales

Avenida Castendo

3550-185 PENALVA DO CASTELO

Contacto Telefónico: 961357250

E-Mail: dpo@cm-penalvadocastelo.pt

b) O Município de Penalva do Castelo acede à informação e procede ao tratamento dos dados pessoais necessários à prestação de serviços abrangida pelo contrato, exclusivamente para esse fim, nos termos da legislação aplicável, assegurando antecipadamente o cumprimento das obrigações previstas no RGPD.

c) O Município de Penalva do Castelo deve fornecer, se requerido, a documentação necessária para demonstrar o cumprimento de todas as suas obrigações e permitir que eventuais verificações, previstas no âmbito do RGPD, sejam realizadas por ele ou por outra entidade credenciada ou por aquela mandatada para o efeito.

d) O Município de Penalva do Castelo deve assegurar que as pessoas autorizadas a processar ou a aceder a dados pessoais, nos termos e para os efeitos das especificações técnicas descritas no contrato, têm os conhecimentos necessários e especializados para aplicar as medidas técnicas e organizativas, de modo que o tratamento que efetuem seja conforme com o RGPD e demais legislação aplicável.

e) O Município de Penalva do Castelo obriga-se a manter os dados pessoais a que tenha acesso estritamente confidenciais, sendo responsável pela utilização dos dados pessoais e pelo cumprimento do dever de sigilo por parte dos respetivos trabalhadores, colaboradores, e entidades públicas ou privadas subcontratadas ou terceiros, quando for o caso.

f) O Município de Penalva do Castelo obriga-se a tomar em consideração os princípios da proteção de dados desde a conceção (Privacy by design) e da proteção de dados por defeito (Privacy by default), no que diz respeito às ferramentas que adquire e utiliza, produtos, aplicações ou serviços prestados por subcontratados.

g) O Município de Penalva do Castelo, no momento da recolha dos dados, para efeitos das operações necessárias a realizar, que possam envolver dados pessoais sob responsabilidade de tratamento da mesma, deve informar os titulares dos dados ou os seus representantes legais.

h) Para efeitos do número anterior, o Município de Penalva do Castelo deve manter os respetivos registos individualizados por titular de dados, por representante legal quando for o caso, por cada operação de tratamento.

i) O Município de Penalva do Castelo no cumprimento do disposto na alínea e) do n.º 3 do artigo 28.º do RGPD deve, no cumprimento da obrigação de responder aos pedidos de exercício de direitos dos titulares dos dados pessoais.

j) Quando os titulares dos dados pessoais, para efeitos de exercício de direitos legalmente protegidos, solicitarem diretamente ao adjudicatário, esclarecimentos sobre questões de privacidade dos sistemas de tratamento de dados, aquele deve enviar os pedidos, em caso de necessidade, para o seguinte endereço de correio eletrónico dpo@cm-penalvadocastelo.pt

k) O Município de Penalva do Castelo através do responsável pelo tratamento de dados, deve notificar de qualquer violação de dados pessoais, que cause impacto nos direitos do titular dos dados, de acordo com os critérios que venham a ser definidos pela autoridade de controlo nacional, num prazo máximo de 24 horas após o conhecimento dos mesmos, através do envio de mensagem para o seguinte endereço de correio eletrónico dpo@cm-penalvadocastelo.pt, acompanhada de toda a documentação relevante a fim de permitir ao Município de Penalva do Castelo, enquanto responsável pelo tratamento de dados, decidir sobre o cumprimento do disposto nos artigos 33.º ou 34.º do RGPD.

l) A informação a disponibilizar pela entidade adjudicatária, deve conter toda a informação requerida pela autoridade de controlo nacional (Comissão Nacional de Proteção de Dados, CNPD) para efeitos de notificação de violação de dados pessoais, conforme informação disponibilizada em:

http://www.cnpd.pt/bin/notifica_rgpd/data_breach.htm

m) O Município de Penalva do Castelo apoia em caso de necessidade, o responsável pelo tratamento de dados, na realização de avaliações de impacto das operações de tratamento previstas sobre a proteção de dados, no âmbito do objeto abrangido pelo contrato, nos termos do RGPD.

n) As avaliações de impacto referidas na alínea anterior atendem ao Regulamento n.º 1/2018, da CNPD relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados (AIPD) publicitado através do Regulamento n.º 798/2018, de 30 de novembro.

o) O Município de Penalva do Castelo compromete-se a implementar as medidas de segurança, previstas nas orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais definidas pela Resolução do Conselho de Ministros n.º 41/2018, de 28 de março e outras medidas específicas que sejam necessárias implementar, nomeadamente as previstas no artigo 32.º do RGPD.

p) O Município de Penalva do Castelo deve disponibilizar, sempre que necessário, a lista dos colaboradores com autorização de acesso aos sistemas e à informação pessoal dos titulares dos dados que se encontrem sob a responsabilidade do mesmo, devendo manter uma cópia das declarações de compromisso de confidencialidade ou de sigilo dos mesmos.

q) O Município de Penalva do Castelo relativamente aos seus sistemas e plataformas informáticos, compromete-se a fornecer ao adjudicatário as instruções específicas que se revelem necessárias ao tratamento de dados pessoais, realizado pelo adjudicatário, abrangidos pelo RGPD e demais legislação aplicável.

r) A contratação, pelo Município de Penalva do Castelo, de outro subcontratante está sujeita à prévia autorização por escrito, geral ou específica da primeira outorgante nos termos do disposto no n.º 2 do artigo 28.º do RGPD.

s) Os direitos O Município de Penalva do Castelo, atendendo à natureza do tratamento de dados pessoais objeto do contrato são os estabelecidos no RGPD e demais legislação aplicável.

t) O Município de Penalva do Castelo colabora com o Data Protection Officer (Encarregado de Proteção de Dados, DPO), facultando todas as informações e esclarecimentos que este vier a solicitar no âmbito das suas funções.

Capítulo III

Penalidades contratuais e resolução

Cláusula 12.^a

Penalidades contratuais

1 – Pelo incumprimento de obrigações emergentes do contrato, a Câmara Municipal de Penalva do Castelo pode exigir ao adjudicatário o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:

a) Pelo incumprimento das datas e prazos da prestação de serviço objecto do contrato, até 10%;

2 – Em caso de resolução de contrato por incumprimento do prestador de serviços, a entidade adjudicante pode exigir-lhe uma pena pecuniária deduzida das importâncias pagas pelo prestador de serviços ao abrigo do número 1, relativamente aos serviços cujo atraso na respectiva conclusão tenha determinado a resolução do contrato.

3 – Na determinação da gravidade do incumprimento, a entidade adjudicante tem em conta, nomeadamente, a duração da infracção, a sua eventual reiteração, o grau de culpa do prestador de serviços e as consequências do incumprimento.

4 – A entidade adjudicante pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos na presente cláusula.

5 – As penas pecuniárias previstas na presente cláusula não obstam a que a entidade adjudicante exija uma indemnização pelo dano excedente.

Cláusula 13.^a

Força maior

1 - Não podem ser impostas penalidades ao prestador de serviços, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respectiva realização, alheias à vontade da parte afectada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.

2 – Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, actos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

3 – Não constituem força maior, designadamente:

a) Circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham;

b) Greves ou conflitos laborais limitados às sociedades do prestador de serviços ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;

c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;

d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;

e) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;

f) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem;

g) Eventos que estejam ou devam estar cobertos por seguros.

4 – A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.

5 - A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afectadas pelo período de tempo comprovadamente correspondente ao impedimento resultante de força maior.

Cláusula 14.^a

Resolução por parte do contraente público

1 – Sem prejuízo de outros fundamentos de resolução do contrato previstos na Lei, a entidade adjudicante pode resolver o contrato, a título sancionatório, no caso de o prestador de serviços violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente nos seguintes casos:

a) Pelo atraso na conclusão dos serviços ou na entrega dos elementos referentes do contrato ou declaração escrita do prestador de serviços de que o atraso respectivo excederá os prazos previstos na cláusula 7.^a.

2 – O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao prestador de serviços e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pelo contraente público.

Cláusula 15.^a

Resolução por parte do prestador de serviços

1 – Sem prejuízo de outros fundamentos de resolução previstos na lei, o prestador de serviços pode resolver o contrato quando:

a) Qualquer montante que lhe seja devido esteja em dívida há mais de seis meses.

2 – Nos casos previstos na alínea a) do n.º 1 desta cláusula, o direito de resolução pode ser exercido mediante declaração enviada à entidade adjudicante, que produz efeitos 30 dias após a recepção dessa declaração, salvo se este último cumprir as obrigações em atraso nesse prazo.

3 – A resolução do contrato nos termos do n.º 1 desta cláusula não determina a repetição das prestações já realizadas pelo prestador de serviços, cessando, porém, todas as obrigações deste ao abrigo do contrato.

Capítulo IV

Resolução de litígios

Cláusula 16.^a

Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo do círculo de Viseu, com expressa renúncia a qualquer outro.

Capítulo V

Disposições finais

Cláusula 17.^a

Subcontratação e cessão da posição contratual

1 – A subcontratação pelo prestador de serviços e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do Código dos Contratos Públicos.

Cláusula 18.^a

Comunicações e notificações

1 – Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.

2 – Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 19.^a

Contagem dos prazos

Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados.

Cláusula 20.^a

Legislação aplicável

A tudo que não esteja especialmente previsto aplica-se o regime previsto no Código dos Contratos Públicos e demais legislação aplicável.

PARTE II – CLÁUSULAS TÉCNICAS

Cláusula 21.^a

Serviços a fornecer

Os serviços a adquirir no âmbito do procedimento pré-contratual que tem por objeto principal o “serviço de segurança e resposta a incidentes” terão de cumprir as características e especificações técnicas constantes nas cláusulas seguintes.

Cláusula 22.^a

Características do serviço

1 - O serviço a prestar compreende o constante no Anexo I deste caderno de encargos.

Penalva do Castelo, 12 de dezembro de 2022.

O Presidente da Câmara,

Francisco Lopes de Carvalho

ANEXO I

CARACTERÍSTICAS TÉCNICAS MÍNIMAS DO SERVIÇO DE SEGURANÇA E RESPOSTA A INCIDENTES

- Os requisitos de segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas e pelos operadores de serviços essenciais, nos termos dos artigos 12.º, 14.º e 16.º do Regime Jurídico da Segurança do Ciberespaço;

-Os requisitos de notificação de incidentes que afetem a segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas, pelos operadores de serviços essenciais e pelos prestadores de serviços digitais, nos termos dos artigos 13.º, 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço, prevendo as circunstâncias, o prazo, o formato e os procedimentos aplicáveis.

Desta forma, pretende-se gerir, controlar, monitorizar, mitigar/bloquear e reportar Incidentes de Segurança Informáticos, bem como dotar a CMPC com capacidade de resposta face a incidentes de segurança, através da deteção, mitigação/bloqueio e resposta a ameaças conhecidas e *zero-day*.

Fornecendo recursos de segurança essenciais para maximizar a visibilidade de segurança e gestão de conformidade: descoberta de ativos, avaliação e análise de vulnerabilidades, correlação de logs/eventos (SIEM), resposta a incidentes, análise de risco, gestão de logs, relatórios de compliance (SOX, ISO27001, RGPD,...), alertas por email, ticketing integrado / alertas, monitorização comportamental, análise forense, monitorização dark web e MSS (*Managed Security Services*);

Deverá fazer menção, quando aplicável, aos métodos e plataformas utilizadas no desenho, implementação e monitorização da solução proposta.

A proposta a apresentar para adoção de medidas técnicas e organizativas destinadas ao cumprimento dos requisitos de segurança previstos no Regime Jurídico da Segurança do Ciberespaço e pelo decreto-lei 65/2021 que obedece ao princípio da adequação e da proporcionalidade, deverá contemplar pelo menos as seguintes atividades:

1 - Avaliação do Sistema de Gestão de Segurança da Informação da Câmara Municipal:

1.1 - Levantamento de situações anómalas;

1.2 - Levantamento de políticas, processos e procedimentos de segurança e resposta a incidentes de segurança;

1.3 - Recolha da informação de registo (logs), providenciando a monitorização aos principais portais, para avaliação de riscos e vulnerabilidades (verificação do estado atual da estrutura de IT);

1.4 - Recolha e monitorização de informação da estrutura IT da Câmara Municipal;

1.5 - Recolha das configurações de *switching* e *routing* (*layer 2* e *3*) para análise das metodologias de segurança utilizadas pela CMPC ao nível de *networking*;

1.6 - Recolha de informação sobre a arquitetura e tecnologias utilizadas em toda a estrutura IT, com principal ênfase na DMZ;

1.7 - Identificação e análise dos ativos de rede;

1.8 - Identificação dos servidores (independentemente do sistema operativo) para verificação de GPOs, portas/protocolos e serviços disponibilizados.

Com a implementação\adoção das medidas atrás referidas deverá ser possível efetuar a seguinte análise:

a) - Uso de tecnologias menos recentes em praticamente todas as áreas de atuação e as políticas de autenticação definidas internamente para determinados processos;

b) - Aplicações WEB que estejam expostas a ataques realizados internamente e externamente;

c) - Dos sistemas ativos de segurança, quais as assinaturas ativas para cada funcionalidade;

d) – DMZ(s) em termos de arquitetura e infraestruturas periféricas. Será feita a análise quanto à performance, ao nível de pedidos executados internamente;

e) - Das políticas e normas de segurança da informação existentes na CMPC, verificação de conformidades;

f) - Forma como são realizadas as atualizações de portais e outros sistemas, bem como a sua manutenção, no sentido de verificar-se a existência de ficheiros com informação sobre instalação de atualizações e que possam fornecer demasiada informação interna;

g) - Regras e políticas configuradas nos sistemas ativos de segurança;

h) - Capacidade de detetar e prevenir ataques, através de equipas de monitorização contra intrusões;

i) - Permissões de acesso à rede, verificando se existe algum controlo sobre os colaboradores para instalação de software;

j) - Existência de protocolos de autenticação segura, bem como de colocação das máquinas em quarentena caso não cumpram com os requisitos de segurança estabelecidos;

k) - Vulnerabilidades existentes nas aplicações e Bases de Dados (com respetivos conectores) independentemente do nível/grau de programação/linguagem utilizada, *frameworks*, sobre as quais estão assentes os respetivos sistemas operativos;

2 - Resposta a Incidentes de Segurança

2.1 - Monitorização em Tempo Real e Análise da Triagem / Incidente

2.2 - Penetration Testing:

Com o objetivo de visualizar o ambiente da CMPC e aumentar a visibilidade do risco de segurança para qual a entidade está exposta

2.3 - Resposta a Incidentes no Local

2.4 - Mapeamento de Rede / *Vulnerability Scanning*

2.5 - Coletar, Reter e Armazenar dados de Auditoria/ Criação e Gestão de Conteúdos de Auditoria

3 - Análise de Vulnerabilidades

3.1 – Análise de segurança de serviços publicados na intranet/internet (independentemente do serviço, aplicação, porta ou protocolo disponibilizado pela CMPC, no sentido de garantir que ataques realizados por *hackers* com intenções maliciosas sejam minimizados, e apoio nas respetivas correções/mitigações a realizar sempre que sejam identificadas vulnerabilidades)

3.2 - Gestão de vulnerabilidades e testes de intrusão

3.3 - Análise aos sistemas e aplicações da CMPC, sobre todos os IP's com serviços ativos publicados pela instituição;

As ferramentas a utilizar para o efeito, serão selecionadas de acordo com os resultados das fases de recolha de informação e de acordo com o conhecimento que se irá gerar com o decorrer dos testes.

Desta forma, para levantamento de vulnerabilidades, análise do risco e execução de testes de intrusão com injeção de incidentes informáticos deverá ser executada em coordenação com a equipa do Gabinete de Informática da CMPC ou entidades terceiras que prestam serviço a este Município.

4 – Desenho e Implementação processual:

4.1 - Identificação do responsável de segurança:

Deverá ser nomeado um elemento da organização, como ponto de contacto com o fornecedor, por forma a serem estabelecidos os canais de comunicação necessários, os procedimentos de notificação, e formalizada a devida nomeação do elemento interno como RESPONSÁVEL DE SEGURANÇA.

Este ponto de contacto da CMPC do ponto de vista técnico/operacional, devendo ser capaz de responder às solicitações da equipa operacional do CNCS (CERT.PT), sendo inclusive esperada disponibilidade para contactos de emergência, fora do horário de expediente;

4.2 - Identificação de funções ou atividades críticas nos processos de negócio na CMPC:

Por forma a identificar as prioridades nos respetivos processos e a criticidade inerente aos seus serviços, esta informação deverá permitir, a partir de eventos de cibersegurança recolhidos de outras fontes, identificar rapidamente possíveis ameaças ou ataques em curso que envolvam a organização e/ou a função ou atividade associada.

Com este procedimento, define-se os processos mais importantes para a CMPC, por forma a ordená-los por criticidade, identificando potenciais ameaças e consequentes impactos, identificando ainda dependências internas e externas entre sistemas;

4.3 - Estabelecimento de canais de comunicação:

No que concerne à troca de informação por correio eletrónico, muita desta informação é bastante sensível. Assim sendo, esta deverá ser encriptada, sendo que todas as partes envolvidas terão as próprias chaves PGP (ou outras a definir).

4.4 - Registo de endereços ip no lir (local internet registry):

Sendo a base de dados do LIR a principal fonte de informação de contacto para a comunidade internacional de resposta a incidentes e para o CNCS em particular, a associação de endereços IP a entidades. A CMPC deverá ter esta informação atualizada perante o LIR, uma vez que permitirá à

organização receber notificações e outra informação de cibersegurança relevante para as redes e sistemas sob a sua responsabilidade.

4.5 - Análise de risco:

A gestão do risco é o processo contínuo de identificação, avaliação e resposta ao risco.

Deverão ser realizadas as análises de risco necessárias, por forma a:

4.5.1 - Identificar as vulnerabilidades associadas a esses serviços e as ameaças a que a que se encontram expostos;

4.5.2 - Calcular a probabilidade de concretização da ameaça e o impacto daí esperado;

4.5.3 - Avaliar a criticidade de cada um dos ativos, baseada no impacto decorrente de uma eventual falha de segurança (nível de risco).

4.6 – Definição de cadeia de responsabilidade:

Deverá ser definida a cadeia de responsabilidade, podendo a mesma ser ajustada ao longo de todo o processo.

Devem ser definidos os privilégios de acesso individual, tendo em conta as funções desempenhadas e as responsabilidades inerentes, sendo posteriormente dado conhecimento a toda a CMPC. Inicia-se com a atribuição da responsabilidade primordial de o Responsável de Segurança detetar os incidentes de cibersegurança dentro da organização, o qual irá definir, diligenciar e aprovar os devidos processos de deteção de incidentes.

4.7 – Política de Segurança:

Será criada a Política de Segurança de Informação adequada à CMPC, atendendo às necessidades e responsabilidades. A sua efetivação verificar-se-á mediante os processos e procedimentos específicos que serão implementados por cada departamento da organização.

4.8 - Procedimentos de notificação de incidentes:

Será elaborado um procedimento de notificação de incidente de cibersegurança, com impacto nas funções ou atividades identificadas como críticas.

5 – Arquitetura de segurança:

De forma a dotar a organização com os principais recursos processuais e técnicos de base para uma defesa eficaz dos seus ativos, quer a nível de perímetro de rede, quer de servidores, postos de trabalho e outros dispositivos deverão ser executadas as seguintes ações:

5.1 - Desenho e implementação da arquitetura e segurança perimétrica:

Com base na análise de risco realizada, irá desenhar-se uma nova arquitetura de cibersegurança para a organização (caso se aplique), por forma a organizar as várias áreas de segurança, identificando as necessidades de deteção de eventos anómalos com origem no exterior e entre zonas de segurança distintas.

5.2 - Implementação de sistema de recolha e armazenamento do fluxo de tráfego, essencial para identificar padrões de comunicação com sistemas potencialmente comprometidos e analisar tráfego considerado malicioso.

5.3 - Comunicação com o cncs, definição de procedimento de comunicação entre a CMPC e o CNCS.

5.4 - Inventariação de ativos / produção de um mapa de redes, bem como a análise do diagrama existente com as principais infraestruturas de comunicações de dados e os sistemas de suporte aos serviços críticos da organização.

5.5 - Verificação da recolha centralizada de registos (logs):

Uma vez que os logs produzidos pelo sistema operativo e pelas aplicações de suporte à atividade, são o principal instrumento de análise e investigação de um incidente de cibersegurança, será verificado se a CMPC possui um repositório central para estes logs, e qual o prazo de armazenamento dos mesmos.

5.6 - Criação de instrumentos de correção ou mitigação de incidentes:

Dependendo da origem do incidente em causa, em que será necessário aplicar medidas corretivas ou de mitigação, serão criados os devidos instrumentos de correção e/ou mitigação.

5.7 - Conformidade com a legislação aplicável e normas da área de atividade:

A organização deve ter sempre presente seja os quadros legais e regulatórios a qua está sujeita, bem como a conformidade com normas ou certificações exigidas por Lei ou por força de exigências contratuais ou regulatórias impostas à atividade da organização, devendo este ser um fator prioritário.

O incumprimento destas normas pode significar perdas de reputação ou de negócios indesejáveis e potencialmente inoportáveis.

Como tal, deverá ser feita uma análise a tais elementos, por forma a atingir a conformidade, com o necessário para a organização.

5.8 - Criação de uma política de uso aceitável(PUA):

Criação da PUA onde estarão consignadas as linhas de orientação para a boa utilização dos recursos TIC internos.

5.9 - Manutenção de infraestruturas de cópias de segurança e reposição (backup/restore):

Criação\revisão de mecanismos proporcionais ao risco existente de eliminação ou corrupção de dados em sistemas que são importantes para o bom funcionamento da organização.

5.10 - AÇÕES DE FORMAÇÃO:

As ações de formação necessárias a consolidar as ações anteriores.

6 – Implementação das medidas propostas:

Deverão contemplar auditorias de segurança e mecanismos de supervisão, bem como a consolidação de informação de registo e monitorização no sistema integrado de gestão de eventos (SIEM).

6.1 - Definição de procedimentos de operação:

Identificação dos procedimentos para a deteção de incidentes, atualização de ativos, triagem, análise de observáveis, fluxo de informação interno e de interação com entidades externas. Serão ainda identificadas as responsabilidades e funções para os procedimentos acima descritos, bem como toda a sua tramitação, consoante a ocorrência em causa, sendo considerados assim diferentes cenários de atuação.

6.2 - Plano de segurança:

Elaboração de um plano de segurança, o qual conterá a política de segurança, descrição das medidas organizativas, formação, identificação do responsável de segurança, bem como a identificação do ponto de contacto permanente para com o CNCS.

6.3 - Auditoria de segurança a bases de dados:

Realização de auditorias de segurança às bases de dados da organização, por forma a atestar que a instalação e a configuração dos mecanismos das fases anteriores estão consoante as necessidades da CMPC.

6.4 - Mecanismos de monitorização:

Instalação e configuração de um sistema de monitorização dos principais ativos de rede e sistemas de suporte às atividades da organização, o qual deverá medir indicadores de disponibilidade e de qualidade dos equipamentos e serviços, despoletando alertas sempre que o valor medido ultrapasse os parâmetros normais de funcionamento (definidos pela organização).

6.5 - Hardening das configurações:

Realização de robustecimento alinhado com um mapeamento das ameaças, das ações de mitigação dos riscos e com a execução das atividades corretivas, com foco na infraestrutura.

6.6 - Security information and event management (siem):

Apoio ao sistema de gestão e correlação de dados e eventos, por forma a facilitar a análise em tempo real e acelerando a tomada de ações defensivos, caso seja necessário.

6.7 - Simulacros de incidentes de cibersegurança:

Realização de pelo menos, um simulacro de um incidente de cibersegurança para avaliação da CMPC.

6.8 - Definição de procedimentos de reação a incidentes:

Identificação dos tipos de ataques mais comuns, criando-se um procedimento para a respetiva mitigação ou resolução, bem como qual o procedimento interno para notificação de incidentes.

6.9 - Testes de aceitação de serviços e mecanismos honeypots:

Deverão ser realizados testes de aceitação de serviços, submetendo as aplicações, serviços e sistemas a ataques de vários tipos e intensidades, por forma a analisar o respetivo comportamento perante esses ataques, propondo as soluções devidas.

6.10 - Resposta a incidentes de segurança

Implementação de Capacidade de Resposta a Incidentes de Segurança, que poderá ser realizada pela CMPC;

7 - Calendarização e Plano de Trabalhos:

Apresentação de calendário com as diversas fases de implementação do projeto.

8 – Duração do contrato de prestação de serviços:

12 meses