



**RENOVAÇÃO DE SOFTWARE NO ÂMBITO
DOS SISTEMAS DE INFORMAÇÃO**

PROC. 163/2022_CMA

- AJUSTE DIRETO -

CADERNO DE ENCARGOS



ÍNDICE

PARTE I - CLÁUSULAS JURÍDICAS.....	3
CAPÍTULO I - DISPOSIÇÕES GERAIS.....	3
CLÁUSULA 1.ª (OBJETO)	3
CLÁUSULA 2.ª (CONTRATO)	3
CLÁUSULA 3.ª (PRAZO CONTRATUAL).....	3
CAPÍTULO II - OBRIGAÇÕES CONTRATUAIS	4
SECÇÃO I - OBRIGAÇÕES DO PRESTADOR DE SERVIÇOS	4
CLÁUSULA 4.ª (OBRIGAÇÕES PRINCIPAIS DO PRESTADOR DE SERVIÇOS)	4
CLÁUSULA 5.ª (CONFORMIDADE E OPERACIONALIDADE DO SOFTWARE)	4
CLÁUSULA 6.ª (MANUTENÇÃO DO SOFTWARE)	5
CLÁUSULA 7.ª (OBJETO DO DEVER DE SIGILO)	5
SECÇÃO II - OBRIGAÇÕES DO MUNICÍPIO DE ALENQUER	5
CLÁUSULA 8.ª(PREÇO BASE)	5
CLÁUSULA 9.ª (PREÇO CONTRATUAL)	6
CLÁUSULA 10.ª (CONDIÇÕES DE PAGAMENTO).....	6
CAPÍTULO III - SANÇÕES CONTRATUAIS E RESOLUÇÃO	6
CLÁUSULA 11.ª (SANÇÕES CONTRATUAIS)	6
CLÁUSULA 12.ª (FORÇA MAIOR)	7
CLÁUSULA 13.ª (RESOLUÇÃO POR PARTE DO MUNICÍPIO DE ALENQUER).....	8
CLÁUSULA 14.ª (RESOLUÇÃO POR PARTE DO PRESTADOR DE SERVIÇOS)	8
CAPÍTULO IV - CAUÇÃO E SEGUROS.....	9
CLÁUSULA 15.ª (CAUÇÃO)	9
CLÁUSULA 16.ª (SEGUROS).....	9
CAPÍTULO V - RESOLUÇÃO DE LITÍGIOS.....	9
CLÁUSULA 17.ª (FORO COMPETENTE)	9
CAPÍTULO VI - DISPOSIÇÕES FINAIS	9
CLÁUSULA 18.ª (SUBCONTRATAÇÃO E CESSÃO DA POSIÇÃO CONTRATUAL).....	9
CLÁUSULA 19.ª (COMUNICAÇÕES E NOTIFICAÇÕES)	9
CLÁUSULA 20.ª (CONTAGEM DOS PRAZOS)	9
CLÁUSULA 21.ª (LEGISLAÇÃO APLICÁVEL)	10
PARTE II CLÁUSULAS TÉCNICAS.....	10
LOTE 1 - Sistema de prevenção proactiva contra intrusão	10
LOTE 2 - Licenciamento VPN	Erro! Marcador não definido.
LOTE 3 - Plataforma Zoom – Plano Profissional	20
LOTE 4 - Serviços Técnicos Especializados	21



PARTE I - CLÁUSULAS JURÍDICAS

CAPÍTULO I - DISPOSIÇÕES GERAIS

O presente contrato rege-se pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, alterado e republicado pelo Decreto-Lei n.º 278/2009, de 2 de outubro, na sua atual redação, doravante designado CCP (Código dos Contratos Públicos).

CLÁUSULA 1.ª (OBJETO)

1 - 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 a celebração de um contrato para a **renovação de software no âmbito dos sistemas de informação**, de acordo com as cláusulas do presente caderno de encargos.

2 - À presente aquisição corresponde a categoria 72600000-6 *Serviços de consultoria e assistência informáticas*, conforme o Regulamento (CE) n.º 213/2008 da Comissão de 28 de novembro de 2007 que altera o Regulamento (CE) n.º 2195/2002 do Parlamento Europeu e do Conselho, relativo ao Vocabulário Comum para os Contratos Públicos (CPV), e as Diretivas do Parlamento Europeu e do Conselho 2004/17/CE e 2004/18/CE, relativas aos processos de adjudicação de contratos, no que respeita à revisão do CPV.

CLÁUSULA 2.ª (CONTRATO)

1 - Quando a redução do contrato a escrito não tenha sido exigida ou tenha sido dispensada, entende-se que o contrato resulta da conjugação do caderno de encargos com o conteúdo da proposta adjudicada.

2 - Fazem sempre parte integrante do contrato, independentemente da sua redução a escrito:

- a) Os suprimientos dos erros e das 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 retificações relativos ao caderno de encargos;
- c) O presente caderno de encargos;
- d) A proposta adjudica;
- e) Os esclarecimentos sobre a proposta adjudicada prestados pelo prestador de serviços.

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

CLÁUSULA 3.ª (PRAZO CONTRATUAL)

1 – O fornecimento e serviços objeto do contrato, devem ser disponibilizados e instalados em conformidade com o presente caderno de encargos, de acordo com as especificações



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

constantes na Parte II do presente caderno de encargos, no prazo de 5 dias, nos locais definidos pelo Município de Alenquer.

2 – O contrato entra em vigor no dia útil seguinte à sua outorga e manter-se-á em vigor pelo prazo de 12 (doze) meses, em conformidade com os respetivos termos e condições, que terá que ser efetuado de acordo com o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

CAPÍTULO II - OBRIGAÇÕES CONTRATUAIS

SECÇÃO I - OBRIGAÇÕES DO PRESTADOR DE SERVIÇOS

CLÁUSULA 4.ª (OBRIGAÇÕES PRINCIPAIS DO PRESTADOR DE SERVIÇOS)

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

- a) Obrigação de entrega, instalação, configuração e formação do software identificado na sua proposta;
- b) Obrigação de garantia e manutenção do software, de acordo com as especificidades definidas no presente caderno de encargos, durante o período de vigência do contrato).
- c) Comunicar antecipadamente ao Município de Alenquer, logo que tenha conhecimento de qualquer facto que torne total ou parcialmente impossível o fornecimento dos bens objeto de contrato, ou o cumprimento de qualquer outra das suas obrigações nos termos do contrato;
- d) Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato.

2 - A título acessório, o cocontratante fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à execução do contrato, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

CLÁUSULA 5.ª (CONFORMIDADE E OPERACIONALIDADE DO SOFTWARE)

1 - O prestador de serviços obriga-se a entregar e instalar ao Município de Alenquer o software objeto de contrato com as características, especificações e requisitos técnicos previstos na parte II do presente caderno de encargos, que dele faz parte integrante.

2 – O software objeto de contrato deve ser entregue e instalado em perfeitas condições de ser utilizado para os fins a que se destina e dotados de todo o material de apoio necessário ao seu funcionamento, bem como a necessária formação.



CLÁUSULA 6.ª (MANUTENÇÃO DO SOFTWARE)

1 - Nos termos do presente artigo, o prestador de serviços garante a manutenção do software durante o período de vigência do contrato.

2 - A manutenção prevista no número anterior abrange:

- a) A atualização de novas versões remotamente;
- b) A deslocação ao local da instalação em caso de não ser possível realizar a manutenção remotamente;
- c) A mão-de-obra.

3 - No prazo máximo de 30 dias a contar da data em que o Município de Alenquer tenha detetado qualquer defeito ou discrepância, este deve notificar o prestador de serviços, para efeitos da respetiva reparação. A notificação deverá realizar-se através de e-mail.

4 - A reparação ou substituição previstas no presente artigo devem ser realizadas dentro de um prazo razoável fixado pelo Município de Alenquer e sem grave inconveniente para este último, tendo em conta a natureza dos equipamentos e o fim a que o mesmo se destina.

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 ao Município de Alenquer, 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 objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.

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

SECÇÃO II - OBRIGAÇÕES DO MUNICÍPIO DE ALENQUER

CLÁUSULA 8.ª(PREÇO BASE)

1 – O preço base é o preço máximo que o Município de Alenquer se dispõe a pagar pela execução de todas as prestações que constituem o seu objeto.

2 – O preço base fixado para o presente contrato é de 13.200,00 € (treze mil e duzentos euros), acrescida de IVA à taxa legal.



CLÁUSULA 9.^a (PREÇO CONTRATUAL)

1 - Pela prestação dos serviços objeto de contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, o Município de Alenquer deve pagar ao prestador de serviços o preço constante da proposta adjudicada, acrescidos de IVA à taxa legal em vigor, se este for legalmente devido, até ao limite do preço contratual, o qual corresponde ao preço base.

2 - O preço referido no número anterior 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, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

CLÁUSULA 10.^a (CONDIÇÕES DE PAGAMENTO)

1 — O pagamento ao prestador de serviços será efetuado de acordo com os preços constantes da proposta adjudicada, acrescidos de IVA à taxa legal em vigor, se este for legalmente devido, até ao limite do preço contratual, o qual corresponde ao preço base.

2 - A quantia devida pelo Município de Alenquer, nos termos da cláusula anterior, deve ser paga no prazo estimado de 30 dias após a receção e validação pelo Município de Alenquer da respetiva fatura, a qual só pode ser emitida após o vencimento da obrigação respetiva.

3 - Em caso de discordância por parte do Município de Alenquer, quanto aos valores indicados na fatura, deve este comunicar ao prestador de serviços, por escrito, os respetivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.

4 - Desde que devidamente emitidas e observado o disposto no n.º 1, a fatura é paga através de transferência bancária.

CAPÍTULO III - SANÇÕES CONTRATUAIS E RESOLUÇÃO

CLÁUSULA 11.^a (SANÇÕES CONTRATUAIS)

1 - Pelo incumprimento de obrigações emergentes do contrato, o Município de Alenquer pode aplicar sanções contratuais, de natureza pecuniária, nos seguintes termos:

- a) Pelo incumprimento das datas e prazos de entrega e/ou instalação dos bens objeto de contrato, até 5% do preço contratual;
- b) Pelo incumprimento da obrigação de garantia técnica, até 10% do preço contratual;



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- c) Pelo incumprimento da obrigação de continuidade de fabrico e de fornecimento, até 5% do preço contratual.

2 - Em caso de resolução do contrato por incumprimento do prestador de serviços, o Município de Alenquer pode exigir-lhe uma pena pecuniária, até 5% do preço contratual.

3 - Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo prestador de serviços ao abrigo da alínea a) do n.º 1, relativamente aos equipamentos objeto do contrato cujo atraso na entrega tenha determinado a respetiva resolução.

4 - Na determinação da gravidade do incumprimento, o Município de Alenquer tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do prestador de serviços e as consequências do incumprimento.

5 - O Município de Alenquer pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos do presente artigo.

6 - As penas pecuniárias previstas no presente artigo não obstam a que o Município de Alenquer exija uma indemnização pelo seu dano excedente.

CLÁUSULA 12.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 respetiva realização, alheias à vontade da parte afetada, 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, atos 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;



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- 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 afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

CLÁUSULA 13.^a (RESOLUÇÃO POR PARTE DO MUNICÍPIO DE ALENQUER)

1 - Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, o Município de Alenquer 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 em caso de atraso, total ou parcial, na entrega e instalação dos equipamentos objeto de contrato superior a um mês ou declaração escrita do prestador de serviços em como o atraso em determinada entrega e instalação excederá esse prazo.

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 Município de Alenquer.

CLÁUSULA 14.^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 em caso de incumprimento de obrigações pecuniárias pelo Município de Alenquer por período superior a seis meses ou quando o montante em dívida exceda 25% do preço contratual, excluindo juros de mora.

2 - Nos casos previstos no número anterior, o direito de resolução pode ser exercido mediante declaração enviada ao Município de Alenquer, que produz efeitos 30 dias após a receção dessa declaração, salvo se este último cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

3 - A resolução do contrato nos termos dos números anteriores não determina a repetição das prestações já realizadas pelo prestador de serviços, cessando, porém, todas as obrigações deste ao abrigo do contrato.

CAPÍTULO IV - CAUÇÃO E SEGUROS

CLÁUSULA 15.^a (CAUÇÃO)

De acordo com o disposto no n.º 2 do artigo 88.º do Código dos Contratos Públicos, não é exigida a prestação de caução no âmbito do presente contrato.

CLÁUSULA 16.^a (SEGUROS)

1 - É da responsabilidade do prestador de serviços a cobertura, através de contratos de seguro, dos riscos inerentes ao fornecimento.

2 – O Município de Alenquer pode, sempre que entender conveniente, exigir prova documental da celebração dos contratos referidos no número anterior, devendo o prestador de serviços fornecê-la no prazo de 5 dias.

CAPÍTULO V - RESOLUÇÃO DE LITÍGIOS

CLÁUSULA 17.^a (FORO COMPETENTE)

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do tribunal administrativo de círculo de Lisboa, com expressa renúncia a qualquer outro.

CAPÍTULO VI - DISPOSIÇÕES FINAIS

CLÁUSULA 18.^a (SUBCONTRATAÇÃO E CESSÃO DA POSIÇÃO CONTRATUAL)

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 19.^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 20.^a (CONTAGEM DOS PRAZOS)

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



CLÁUSULA 21.ª (LEGISLAÇÃO APLICÁVEL)

Em tudo o que não esteja especialmente previsto no presente caderno de encargos, o contrato é regulado pelo Código dos Contratos Públicos aplicando-se o artigo 280.º do mesmo.

PARTE II CLÁUSULAS TÉCNICAS

Sistema de Cibersegurança

Especificações técnicas a satisfazer.

1. Descrição Geral.

Os testes a executar aos serviços publicados na web devem seguir uma abordagem black-box, ficando a aguardar o fornecimento de sources, informação de serviços e contas standard, caso seja necessário testar Apps específicas. A abordagem deve refletir todos os protocolos, portas, apps e serviços publicados através dos IPs públicos da Câmara Municipal de Alenquer, através da execução de:

- Testes Network Vulnerability;
- Testes Web Application Vulnerabilities;
- Testes aplicacionais exaustivos.

2. Descrição específica - Análise de vulnerabilidades e injeção de incidentes de segurança. PTES (Penetration Testing Execution Standard).

O serviço deverá incidir sobre todos os serviços publicados nos IPs públicos, podendo ser alterado em função de vulnerabilidades que possam vir a ser identificadas e/ou solicitações por parte da Câmara Municipal de Alenquer, sendo que os testes devem ser feitos a partir da Internet (deverão ser identificados os IPs públicos a partir do qual serão executados os testes).

As ferramentas a utilizar devem ser 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, será necessário a realização de um conjunto de fases exploratórias, que devem ser culminadas com a injeção de exploits recolhidos a partir de Bases de Dados partilhadas em redes públicas (web) e privadas (Tor) e exploits zero-day/zero-hour, cujas assinaturas das plataformas de segurança de perímetro são inexistentes (ou seja, será útil para testar heurísticamente/comportamental os mecanismos de segurança).

Para tal, a entidade deve seguir o standard PTES, dividido nas seguintes secções:



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- Pre-engagement Interactions;
 - Intelligence Gathering;
 - Threat Modeling;
 - Vulnerability Analysis;
 - Exploitation;
 - Post Exploitation;
 - Reporting.
-
- **Recolha de Informação Passiva:** nesta fase devem ser utilizados portais de internet especializados, motores de busca e redes sociais, de forma a recolher informação que possa vir a ser útil sobre os portais, serviços, tecnologias, colaboradores e/ou utilizadores e utilizadas diversas ferramentas de obtenção passiva de informação. A título de exemplo devem ser utilizados, entre outros, os seguintes portais: archive.org, whois.ripe.net, netcraft.com e browserspy.dk. Devem ser ainda utilizadas diversas ferramentas de obtenção passiva de informação, como: Casefile, Creepy, Dmitry, Jigsaw, Maltego, Metagoofil, TheHarvester, Twofi, URLcrazy.
 - **Recolha de Informação Ativa:** nesta fase devem ser feitos acessos diretos, não ofensivos, aos diversos portais e serviços online, de forma a melhor identificar e confirmar as tecnologias utilizadas. De acordo com as especificidades dos portais, devem ser igualmente efetuados testes manuais, de forma a obter informação que escape a ferramentas automáticas. Para além de processos manuais, devem ser utilizadas, entre outras, as seguintes ferramentas: Apache-users, Burpsuite, Dmitry, dnsenum, dnmap, dnsmap, dnsrecon, dnstracer, dnswalk, fierce, fping, fragroute, fragrouter, hydra, ikescan, Maltego, Medusa, nbtscan, ncat, Netdiscover, NMap, smtp-user-enum, sslscan, sslyze, swaks, sslcaudit, ssldump, sslscan, sslyze, tlssled, ua-tester, urlcrazy, wafw00f, Webscarab.
 - **Identificação de vulnerabilidades em servidores e aplicações Web:** após efectuado o levantamento de toda a informação de forma passiva e activa, devem ser efetuados testes customizados às tecnologias identificadas nos servidores e portais Web. Os pontos a testar vão depender do que for identificado nas fases de recolha de informação, bem como em resultados que surjam nesta mesma fase, mas de forma genérica devem ser testadas, quando aplicável, vulnerabilidades Cross Site Scripting (XSS), Blind Structured Query Language Injection (Blind SQLi), SQLi, vulnerabilidades em Procedural Language/Structured Query Language (PL/SQL), análise de vulnerabilidades Remote File Inclusion (RFI), Cookies, Javascript, Applets, Código Flash, Certificados Digitais,



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

Fuzzing (IP, TCP, UDP, cookies, forms, variáveis via URL encoding) entre outras que sejam aplicáveis à tecnologia utilizada pela instituição. De forma a identificar as vulnerabilidades devem ser utilizadas por exemplo, as seguintes ferramentas: Acunetix Web Vulnerability Scanner, AppScan, bbqsql, Casefile, JoomScan, Maltego, NMAP, Nessus, openVAS, Oscanner, Powerfuzzer, sfuzz, spike, SQLninja, SQLmap, WebScarab, wfuzz. Os testes irão obedecer na íntegra ao definido no Caderno de Encargos.

- Identificação de vulnerabilidades em outros serviços como SNMP/POP3/IMAP, NTP, DNS, SSH entre outros: após efetuado o levantamento de toda a informação de forma passiva e ativa, devem ser efetuados testes customizados às tecnologias identificadas nos servidores. Algumas das ferramentas a usar devem ser as seguintes: Bursuite, DNSspoofer, Maltego, Nessus, NMap, openVAS.
- Exploitation Zero-day/Zero-hour: Caso sejam descobertas vulnerabilidades e de forma a eliminar falsos positivos, deverá ser simulado em ambiente lab em condições aproximadas, de forma a validar se se confirmam as falhas identificadas e qual a sua severidade. Além disso, deverá ser realizado o desenvolvimento de código em python, Perl, Ruby e PHP (código que será entregue com os relatórios) que demonstre a usabilidade das vulnerabilidades detetadas, caso não exista nenhum disponível publicamente quer em bases de dados na Internet, quer através de ferramentas Open Source e/ou comerciais, no sentido de testar heurísticamente as soluções e mecanismos de segurança. Em caso de utilização de exploits públicos, devem ser utilizados, entre outros, o portal: exploit-db.com e as ferramentas: Metasploit, Nessus, Netsparker, SQLmap, SQLninja e w3af.
- Testes de intrusão: Sempre que seja confirmada alguma vulnerabilidade crítica, a Câmara Municipal de Alenquer deverá ser prontamente informada, de forma a minimizar o tempo de exposição à falha de segurança (categorizada como vulnerabilidade Muito Grave ou Grave). Os testes de intrusão devem ser executados à medida que forem identificadas vulnerabilidades que permitam a sua execução.

Licenciamento VPN

Especificações técnicas a satisfazer.

Integração com redes de comunicações.

As seguintes funcionalidades deverão ser suportadas:

- Servidor de DHCP, NTP e DNS incluído.



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- Funcionalidade de DNS Proxy.
- Múltiplos modos de configuração de interfaces:
 - Sniffer.
 - agregação de portas (802.3ad).
 - Loopback.
 - VLANs (802.1Q e trunk).
 - Hardware e software switch (Depende do modelo).
- Routing estáticos e baseado em políticas (PBR - Policy Based Routing).
- Balanceamento e redundância de múltiplos links.
- Suporte para protocolos de routing dinâmico: RIPv1 e RIPv2, OSPFv2 e OSPFv3, ISIS, BGP4.
- Suporte de tráfego multicast: PIM, sparse e dense mode.
- Routing baseado em conteúdos: WCCP e ICAP.
- Proxy explícito.
- Suporte de IPv6.
- Gestão por IPv6.
- Protocolos de routing IPv6.
- Tunneling de IPv6.
- Processamento firewall e UTM de IPv6.
 - NAT64.
 - NAT46.
 - VPN IPSec IPv6.
- Suporte Dual Stack IPv4 e IPv6 em simultâneo.
- Controlador Wireless integrado.

Identificação de utilizadores e dispositivos

As seguintes funcionalidades deverão ser suportadas:

- Base de dados local de utilizadores.
- Autenticação de utilizadores em servidores remotos: LDAP, RADIUS, TACACS+.
- Sistema de Single Sign-on de utilizadores:
 - Windows AD.
 - Novell eDirectory.
 - FortiClient.
 - Citrix e Terminal Server.
 - Radius (accounting message).
 - Autenticação de utilizadores no acesso (802.1x, portal cativo).
- PKI e certificados:
 - certificados X.509.
 - suporte SCEP.
 - criação de Certificate Signing Request (CSR).



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- autorrenovação de certificados antes da data de expiração.
- suporte OCSP.
- Autenticação de 2 fatores:
 - Servidor integrado de autenticação por tokens físicos, tokens por software e SMS.
 - Integração com terceiras partes.
- Identificação de dispositivos:
 - reconhecimento de dispositivo e sistema operativo.
 - classificação de dispositivos automática.
 - gestão de inventário de dispositivos.
- Implementação de políticas de segurança com base em utilizar ou dispositivos.

Firewall

As seguintes funcionalidades deverão ser suportadas:

- Modos de operação NAT/route e transparente/bridge.
- Agendamento de políticas: recorrentes ou apenas uma vez
- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 O, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle).
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pin holing.
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP.
- Visualização de políticas de forma global ou por secção.
- Definição de objetos para utilização em políticas incluindo: predefinidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos.
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de IPs, Geografia e FQDN.
- Configuração de NAT: por política e tabela central de NAT.
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT, STUN.
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (TOS) e Differentiated Services (DiffServ).

VPN

As seguintes funcionalidades deverão ser suportadas:

- IPSEC VPN:
- Suporte para peers remotos: clientes dialup compatíveis com IPSEC, peers com IP estático ou DNS dinâmico;
- Mecanismos de autenticação: certificados ou pre-shared key;
- IPSEC Phase 1 mode: aggressive e main (ID protection) mode;
- Opções de aceitação de peers: qualquer ID, ID específico, ID num grupo de utilizadores dialup;



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- Suporte de IKEv1, IKEv2 (RFC 4306);
- Suporte de IKE mode configuration (como servidor ou cliente), DHCP over
- IPSEC;
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256;
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512;
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14;
- Suporte XAuth como cliente ou servidor;
- XAuth para clientes dialup: Server type option (PAP, CHAP, Auto), NAT Traversal option;
- Duração configurável da chave de encriptação IKE e da frequência do NAT
- traversal keepalive;
- Dead peer detection;
- Replay detection;
- Autokey keep-alive na Phase 2 SA;
- Implementação de VPNs IPSEC nos seguintes modos: gateway-to-gateway, hub- and-spoke, full mesh, redundant-tunnel, terminação de VPNs em modo transparente;
- Opções de configuração de VPNs IPSec: baseado em routing(route-based) ou baseado em políticas (policy-based);
- VPNs SSL:
 - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (bookmarks) mecanismos de ligação, download de cliente;
 - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho;
 - Atalhos (bookmarks) com single sign-on: permite reutilizar um login anterior ou credenciais pré-definidas para aceder a recursos internos;
 - Gestão de atalhos (bookmarks) pessoais;
 - Gestão de utilizadores concorrentes;
 - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso;
 - Suporte de VPN SSL em modo web:
 - para clientes remotos equipamentos apenas com um browser web;
 - disponibiliza suporte web para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, Citrix;
 - Suporte para VPN SSL em modo túnel:
 - Para acesso a partir de computadores que necessitam utilizar qualquer software do tipo cliente-servidor;
 - Disponível para MAC OSX, Linux, Windows.
 - Suporte para VPN SSL em modo port-forwarding:
 - Utiliza uma applet Java para permitir uma utilização alargada de aplicações do tipo cliente-servidor.



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- Validação da integridade do dispositivo cliente e do sistema operativo;
- Opção para limpeza de cache aquando da terminação da sessão VPN SSL;
- Opção de utilização de desktop virtual que permite isolar a sessão VPN SSL no ambiente de trabalho do computador cliente.
- Monitorização de VPNs IPSec e SSL com diferentes níveis de detalhe;
- Suporte para outras VPNs como L2TP (modo cliente e servidor), L2TP over IPSec, PPTP e GRE over IPSec.

IPS - Detecção e prevenção de intrusões

As seguintes funcionalidades deverão ser suportadas:

- Suporte de IPS com mais de 7000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, update de assinaturas manual ou automático (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados;
- Diferentes ações de IPS: definido por defeito na assinatura, monitorizar, bloquear, reset de sessão ou quarentena (IP do atacante, IP de atacante e vítima, interface de entrada) com definição de duração;
- •Possibilidade de registo integral do pacote onde foi detetado o ataque;
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo);
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade;
- Opção de excluir a aplicação de assinaturas de IPS específicas com base em IPs;
- Proteção DOS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination);
- Possibilidade de implementação de IDS em modo sniffer.

Controlo de aplicações

As seguintes funcionalidades deverão ser suportadas:

- Deteção de mais de 3100 aplicações distintas organizadas por categorias;
- Definição de aplicações customizadas;
- Controlo avançado de aplicações de IM e Facebook;
- Definição de diferentes perfis de controlo de aplicações de forma manual ou baseada em filtro (categoria, popularidade, tecnologia, fabricante, risco e/ou protocolo);
- Aplicação de perfis de controlo de aplicações por política de firewall para maior flexibilidade;
- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização, aplicação de gestão de largura de banda;
- Inspeção SSH.



Proteção contra ameaças

As seguintes funcionalidades deverão ser suportadas:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, antivírus, filtragem WEB e DLP.
- Detecção e bloqueio de BOTNETs com base em listas de reputação de IPs globais.
- Suporte de antivírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões).
- Suporte de inspeção de antivírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP.
- Suporte de antivírus em modo proxy, incluindo:
 - Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP.
 - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox).
 - Listas de ficheiros autorizados/negados.
 - Opção de análise heurística.
- Detecção de sites WEB (web filtering):
 - Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS).
 - Possibilidade de definição manual de filtragem sites com base em URL, conteúdo web e cabeçalho MIME.
 - Categorização dinâmica em tempo real, baseada na cloud, com mais de 250 milhões de sites categorizados, de 70 idiomas e organizados em mais de 77 categorias.
 - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter.
 - Deverá ser possível ter a opção para ativar as seguintes funcionalidades:
 - Filtrar Java Applet, ActiveX e/ou cookies.
 - Bloquear HTTP Post.
 - Registrar termos/palavras utilizados nas pesquisas em motores de busca.
 - Identificar imagens pelo URL.
 - Bloquear redirect de HTTP de acordo com a categoria.
 - Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores.
 - Definição de quotas de utilização WEB com base em categorias.
 - Definição de categorias customizada e sobreposição de categorização.
 - Mecanismos de exceção à utilização de perfis pré-definidos.
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS.

- Prevenção e proteção de fugas de informação – DLP:
- Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP:
 - Possibilidade de executar as ações: registar, bloquear, quarentena de utilizar/IP/Interface.
 - Filtros pré-definidos incluindo cartões de crédito e número de segurança Social.
- Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP:
 - Opções de filtragem disponíveis, tais como tamanho, tipo de ficheiro, watermark, conteúdo e deteção de encriptação.
- Utilização de mecanismos de DLP watermarking, com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux.
- Fingerprinting de ficheiros.
- Arquivamento de ficheiros detetado para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB.

Controlo de Endpoints

As seguintes funcionalidades deverão ser suportadas:

- Gestão de dispositivos de rede através de software cliente:
- Suporte de Windows, MAC OSX, Android e iOS;
- Validação de postura: garantir que a instalação de software no cliente e várias definições estão de acordo com o pretendido;
- Provisionamento de configuração de cliente: atualização automática de configurações do cliente, tais como VPN e definições de filtragem WEB;
- Perfis de segurança específicos para equipamentos off-net (fora de rede protegida, por exemplo portáteis em mobilidade);
- Implementação de registo de atividade dos clientes.

Alta disponibilidade

As seguintes funcionalidades deverão ser suportadas:

- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP,
- Interfaces de heartbeat redundantes,
- Interfaces reservadas para gestão,
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade,
- Reposição automática de serviço (failover),
- Monitorização de portas e links (locais e remotos).



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- Sem perda de sessões.
- Failover em menos de 1 segundo.
- Notificações de eventos de failover.
- Diferentes opções de arquitetura:
 - HA com agregação de links.
 - Full mesh HA.
 - Suporte para HA com equipamento geograficamente dispersos.
- Opção de sincronização de sessões em equipamentos configurações em modo Standalone.

Administração, Monitorização e Diagnósticos

As seguintes funcionalidades deverão ser suportadas:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser.
- Acesso de gestão em modo de texto: SSH, Telnet ou consola.
- Sem necessidade de utilização de software cliente específico para gestão gráfica.
- Suporte de múltiplas linguagens de administração no acesso gráfico, incluindo: Português, Inglês, Espanhol, Francês, Japonês, Chinês simplificado, Chinês tradicional e Coreano.
- Suporte para gestão local e gestão centralizada em simultâneo.
- Suporte para gestão centralizada com integração em plataforma específica para o efeito.
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog.
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts.

Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.

Registo de eventos e relatórios

As seguintes funcionalidades deverão ser suportadas:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória e/ou disco rígido locais, múltiplos servidores de syslog, múltiplos servidores específicos
- para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e
- plataformas disponíveis na cloud.
- Opção de logging confiável com recurso a mecanismos TCP (RFC 3195).
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas.
- Possibilidade de exportar relatórios em formato PDF.
- Calendarização de backups de logs para sistemas externos.



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos.
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, Wireless.
- Opção para registo encurtado ou completo de eventos.
- Resolução de nomes de endereços IPs e protocolos.

Certificações

O equipamento deverá ter as seguintes certificações:

- Certificações ICSA de Firewall, SSL VPN, IPSEC VPN, AV e IPS.
- FIPS 140-2 Validated (quando a operar em FIPS mode).
- USGv6 IPv6 Certified.

Plataforma Zoom – Plano Profissional

Especificações técnicas a satisfazer.

Zoom é uma plataforma de vídeo e áudio conferência online para empresas, profissionais e coletivos que necessitam manter reuniões sem que a distância seja um impedimento. Zoom funciona diretamente desde o navegador, mas também conta com app para iPhone/iPad, app Android, complemento de Outlook e extensões para navegador.

Para começar a usar Zoom o único requisito é criar uma conta na plataforma, pode partir da modalidade gratuita e posteriormente subscrever-se à modalidade de pagamento que mais se ajusta às suas necessidades. A modalidade gratuita tem limitações de participantes e tempo por sessão, mas é útil para testar a qualidade de áudio e imagem da plataforma.

Existem diferentes tarifários para o uso de Zoom, partindo do primeiro que é gratuito, dá para ter uma ideia de como funciona e qual a qualidade. De seguida apresentamos de forma resumida as principais diferenças entre os planos de licença.

Plano Profissional - Ideal para equipas pequenas.

Caraterísticas fundamentais da Plataforma Zoom - Plano Profissional:

- Suporte telefónico exclusivo
- Suporte administrativo
- Direção personalizada URL da empresa
- Domínios administrados
- Ingresso individual



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

- Marca da empresa
- Correios eletrónicos personalizados
- Integração com LTI

Serviços Técnicos Especializados

Especificações técnicas a satisfazer.

Os serviços profissionais serão realizados através dos seguintes meios. Estes serão aplicados às tecnologias de segurança instaladas no Município de Alenquer:

- Telefónico através de uma linha de apoio (requisição e prestação do serviço);
- Correio eletrónico (requisição e prestação do serviço);
- Suporte online através do site de suporte (requisição do serviço);
- Acesso remoto (prestação do serviço);
- Presencial (prestação do serviço).

Recuperação de sistemas de segurança, sempre que possível, devido à degradação dos mesmos por:

- Manipulação indevida - operações executadas sobre os ficheiros fora do contexto dos sistemas (por exemplo, via GUI de sistema, etc.);
- Limitações / deficiente gestão do espaço em disco - limitações da configuração do sistema de segurança com deficiente gestão do espaço em disco devido a outras utilizações do sistema;
- Não obediência aos procedimentos de obtenção de cópias de segurança;
- Quebra do sistema lógico de segurança (sistema de controlo de acessos) - acesso fraudulento por utilizadores não reconhecidos do sistema;
- Tentativas de violação de "copyright";
- Falhas de segurança física - por deficiente ou inexistente equipamento de segurança física; por deficiente funcionamento do próprio equipamento informático.

Necessidades de modificar a funcionalidade das tecnologias de segurança por:

- Necessidade de possuir mais operações disponíveis;
- Alterações à funcionalidade das operações existentes;
- Alterações de écrans de entrada de dados e "outputs";
- Redimensionamento de estruturas de dados;
- Outras necessidades definidas pelo Município de Alenquer.



RENOVAÇÃO DE SOFTWARE NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO.

Reinstalação de tecnologias de segurança em novos sistemas (configuração): necessidade de migração plataformas de segurança para novas máquinas com outras dimensões, implicando mesmo assim alterações de parâmetros de instalação.

Condições excepcionais de funcionamento do sistema: procura de solução e acompanhamento em situações de exceção de utilização das tecnologias de segurança.

Elaboração de pareceres técnicos no domínio da segurança em sistemas de informação, quando expressamente solicitados.

As horas-técnico despendidas no âmbito do presente contrato serão reportadas ao Município de Alenquer através de relatórios com uma periodicidade mensal.