

CADERNO DE ENCARGOS RELATIVO A CONTRATOS DE AQUISIÇÃO DE EQUIPAMENTO PARA O REPOSITÓRIO DIGITAL

Capítulo I

Disposições gerais

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 aquisição de equipamentos informáticos e respetivos softwares para o projeto de Repositório Digital do Município de Abrantes, conforme o Anexo I “Características, Requisitos e Especificações Técnicas”.
2. O objeto do contrato abrange ainda serviços de suporte e manutenção conforme o disposto no Anexo I “Características, Requisitos e Especificações Técnicas”.

Cláusula 2.ª

Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2. O contrato a celebrar integra ainda os seguintes elementos:
 - a) Os suprimentos 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 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 respetiva prevalência é determinada pela ordem pela qual aí são indicados.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma legal.
5. Em cumprimento do disposto no artigo 290.º-A do Código dos Contratos Públicos, o acompanhamento da execução do contrato será assegurado pelo colaborador Cláudio Branco de Vasconcelos, enquanto Gestor(a) de Contrato.

Cláusula 3.ª

Prazo

1. O contrato mantém-se em vigor pelo prazo de 3 anos em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do Contrato.
2. O início do contrato conta-se a partir da data de assinatura do mesmo e após publicação no Portal da Internet dedicado aos contratos públicos, sendo condição de eficácia do respetivo contrato esta publicação.

Capítulo II

Obrigações contratuais

Secção I

Obrigações do fornecedor

Cláusula 4.ª

Obrigações principais do fornecedor

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 fornecedor as seguintes obrigações principais:
 - a) Obrigação de entrega dos bens identificados na sua proposta;
 - b) Obrigação de garantia dos bens;
 - c) Obrigação de continuidade de fabrico;
 - d) Obrigação de suporte e manutenção de acordo com o disposto no Anexo I “Características, Requisitos e Especificações Técnicas”.

Cláusula 5.ª

Conformidade e operacionalidade dos bens

1. O fornecedor obriga-se a entregar ao contraente público os bens objeto do contrato com as “Características, Requisitos e Especificações Técnicas” previstas no Anexo I, ao presente Caderno de Encargos, que dele faz parte integrante.
2. Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.
3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens.
4. O fornecedor é responsável perante o Município de Abrantes por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

Cláusula 6.ª

Entrega dos bens objeto do contrato

1. Os bens objeto do contrato devem ser entregues em Praça Raimundo Soares, 2200-366 Abrantes, no prazo de 3 (três) semanas.
2. O fornecedor obriga-se a disponibilizar, simultaneamente com a entrega dos bens objeto do contrato, todos os documentos, que sejam necessários para a boa e integral utilização ou funcionamento daqueles.
3. Com a entrega dos bens objeto do contrato, ocorre a transferência da posse e da propriedade daqueles para o contraente público, bem como, do risco de deterioração ou perecimento dos mesmos, sem prejuízo das obrigações de garantia que impendem sobre o fornecedor;
4. Todas as despesas e custos com o transporte dos bens objeto do contrato e respetivos documentos para o local de entrega, com a respetiva instalação, são da responsabilidade do fornecedor.

Cláusula 7.ª

Verificações

1. Efectuada a entrega dos bens objeto do contrato, o contraente público, por si ou através de terceiro por ele designado, procede, no prazo de 10 dias, à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar, respetivamente, se os mesmos correspondem às quantidades estabelecidas no Anexo I “Características, Requisitos e Especificações Técnicas” ao presente Caderno de Encargos e se reúnem as características, especificações e requisitos técnicos e operacionais definidos no Anexo I “Características, Requisitos e Especificações Técnicas” presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.

Cláusula 8.ª

Inoperacionalidade, defeitos ou discrepâncias

1. No caso de os testes previstos na cláusula anterior não comprovarem a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as

exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no Anexo I “Características, Requisitos e Especificações Técnicas” ao presente Caderno de Encargos, o Município de Abrantes deve de isso informar, por escrito, o fornecedor.

2. No caso previsto no número anterior, o fornecedor deve proceder, à sua custa e no prazo razoável que for determinado pelo Município de Abrantes, às reparações ou substituições necessárias para garantir a operacionalidade dos bens e o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
3. Após a realização das reparações ou substituições necessárias pelo fornecedor, no prazo respetivo, o Município de Abrantes procede à realização de novos testes de aceitação, nos termos da cláusula anterior.

Cláusula 9.ª

Aceitação dos bens

1. Caso os testes a que se refere a Cláusula 7.ª comprovem a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais e neles não sejam detetados quaisquer defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no Anexo I “Características, Requisitos e Especificações Técnicas” ao presente Caderno de Encargos, deve ser emitido, no prazo máximo de 5 dias a contar do final dos testes, um auto de receção, assinado pelos representantes do fornecedor e do Município de Abrantes.
2. Com a assinatura do auto a que se refere o número anterior, ocorre a transferência da posse e da propriedade dos bens objeto do contrato para o Município de Abrantes, bem como do risco de deterioração ou perecimento dos mesmos, sem prejuízo das obrigações de garantia que impendem sobre o fornecedor.
3. A assinatura do auto a que se refere o n.º 1 não implica a aceitação de eventuais defeitos ou de discrepâncias dos equipamentos objeto do contrato com as exigências legais ou com as características, especificações e requisitos técnicos previstos no Anexo I “Características, Requisitos e Especificações Técnicas” ao presente Caderno de Encargos.

Cláusula 10.ª

Garantia técnica

1. Nos termos da presente cláusula e da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, o fornecedor garante os bens objeto do contrato, pelo prazo de 3 anos a contar da data entrega dos bens, contra quaisquer defeitos ou discrepâncias com as exigências legais e com características, especificações e requisitos técnicos definidos no Anexo I “Características, Requisitos e Especificações Técnicas” ao presente Caderno de Encargos, que se revelem a partir da respetiva aceitação do bem.
2. A garantia prevista no número anterior abrange:
 - a) O fornecimento, a montagem ou a integração de quaisquer peças ou componentes em falta;
 - b) A desmontagem de peças, componentes ou bens defeituosos ou discrepantes;
 - c) A reparação ou a substituição das peças, componentes ou bens defeituosos ou discrepantes;
 - d) O fornecimento, a montagem ou instalação das peças, componentes ou bens reparados ou substituídos;
 - e) O transporte do bem ou das peças ou componentes defeituosos ou discrepantes para o local da sua reparação ou substituição e a devolução daqueles bens ou a entrega das peças ou componentes em falta, reparados ou substituídos;
 - f) A deslocação ao local da instalação ou de entrega;
 - g) A mão-de-obra;
 - h) Outros aspetos previstos no Anexo I “Características, Requisitos e Especificações Técnicas”.
3. No prazo máximo de dois meses a contar da data em que o Município de Abrantes tenha detetado qualquer defeito ou discrepância, este deve notificar o fornecedor, para efeitos da respetiva reparação.
4. A reparação ou substituição previstas na presente cláusula devem ser realizadas dentro de um prazo razoável fixado pelo Município de Abrantes, no Anexo I “Características, Requisitos e Especificações Técnicas”, e sem grave inconveniente para este último, tendo em conta a natureza do bem e o fim a que o mesmo se destina.

Subsecção II

Serviços

Cláusula 11.^a

Suporte e Manutenção

1. O fornecedor fica obrigado a prestar serviços de suporte e manutenção durante os prazos previstos no Anexo I “Características, Requisitos e Especificações Técnicas”, contar da data da assinatura do auto de receção respetivo.

Subsecção III

Dever de sigilo

Cláusula 12.^a

Objeto do dever de sigilo

1. O fornecedor deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao Município de Abrantes, 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 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 respetiva 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 outras entidades administrativas competentes.

Cláusula 13.^a

Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor até ao termo do prazo de 10 anos a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Secção II

Obrigações do Município de Abrantes

Cláusula 14.ª

Preço Base

1. Nos termos e para os efeitos do disposto no art. 47.º do CCP, o preço base (máximo) do procedimento, como parâmetro base (máximo) do preço contratual, é fixado em 152.800,00 €, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.

Cláusula 15.ª

Preço contratual

1. Pelo fornecimento dos bens objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o Município de Abrantes deve pagar ao fornecedor 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 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, nomeadamente os relativos ao transporte dos bens objeto do contrato para o respetivo local de entrega, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 16.ª

Condições de pagamento

1. As quantias devidas pelo Município de Abrantes, nos termos das cláusulas anteriores, devem ser pagas no prazo de 60 dias após a receção pelo Município de Abrantes das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. Para os efeitos do número anterior, a obrigação considera-se vencida do seguinte modo:
 - a. Para a 1.ª prestação (um terço do valor total adjudicado): após a aceitação dos bens;

- b. Para a 2.ª prestação (um terço do valor total adjudicado) em 2021 após emissão da Requisição externa;
 - c. Para a 3.ª prestação (um terço do valor total adjudicado) em 2022 após emissão da requisição externa.
- 3. As faturas deverão ser enviadas para o email faturacao@cm-abrantes.pt , com a indicação do número da requisição ou do compromisso.
 - 4. Em caso de discordância por parte do Município de Abrantes, quanto aos valores indicados nas faturas, deve este comunicar ao fornecedor, por escrito, os respetivos fundamentos, ficando o fornecedor obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
 - 5. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas são pagas através de cheque ou transferência bancária.

Capítulo III

Penalidades contratuais e resolução

Cláusula 17.ª

Penalidades contratuais

- 1. Pelo incumprimento de obrigações emergentes do contrato, o Município de Abrantes pode exigir do fornecedor 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 de entrega dos bens objeto do contrato, até 20% do montante da adjudicação;
 - b) Pelo incumprimento da obrigação de garantia técnica, até 25% do montante da adjudicação;
- 2. Em caso de resolução do contrato por incumprimento do fornecedor, o Município de Abrantes pode exigir-lhe uma pena pecuniária de até 25% do montante da adjudicação.
- 3. Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pelo fornecedor ao abrigo da alínea a) do n.º 1, relativamente aos bens objeto do contrato cujo atraso na entrega tenha determinado a respetiva resolução.

4. Na determinação da gravidade do incumprimento, o Município de Abrantes tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do fornecedor e as consequências do incumprimento.
5. O Município de Abrantes pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.
6. As penas pecuniárias previstas na presente cláusula não obstam a que o Município de Abrantes exija uma indemnização pelo dano excedente.

Cláusula 18.ª

Força maior

1. Não podem ser impostas penalidades ao fornecedor, 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 fornecedor, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do fornecedor 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 fornecedor de deveres ou ónus que sobre ele recaiam;

- d) Manifestações populares devidas ao incumprimento pelo fornecedor de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do fornecedor 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 fornecedor 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 19.ª

Resolução por parte do contraente público

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, o Município de Abrantes pode resolver o contrato, a título sancionatório, no caso de o fornecedor violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente nos seguintes casos:
 - a) Atraso, total ou parcial, na entrega dos bens objeto do contrato superior a três meses ou declaração escrita do fornecedor de que o atraso em determinada entrega excederá esse prazo.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao fornecedor e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pelo Município de Abrantes.

Cláusula 20ª

Resolução por parte do fornecedor

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o fornecedor pode resolver o contrato quando:
 - a) Qualquer montante que lhe seja devido esteja em dívida há mais de 6 meses;
2. O direito de resolução é exercido por via judicial, nos termos da Cláusula 21.ª.
3. Nos casos previstos na alínea a) do n.º 1, o direito de resolução pode ser exercido mediante declaração enviada ao Município de Abrantes, 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.
4. A resolução do contrato nos termos dos números anteriores não determina a repetição das prestações já realizadas pelo fornecedor, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444.º do Código dos Contratos Públicos.

Capítulo VI

Resolução de litígios

Cláusula 21.ª

Foro competente

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

Capítulo VII

Disposições finais

Cláusula 22.ª

Subcontratação e cessão da posição contratual

2. A subcontratação pelo fornecedor e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do Código dos Contratos Públicos.

Cláusula 23.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 24.ª

Contagem dos prazos

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

Cláusula 25.ª

Legislação aplicável

2. O contrato é regulado pela legislação portuguesa.

ANEXO I

Características, Requisitos e Especificações Técnicas

Upgrade Servidores:

Pretende-se o upgrade dos servidores existentes (Dell EMC PowerEdge R810 e R820) com placa de rede a 10Gb/s e Placa de Fibra FC a 16Gb/s. As placas a propor deverão ser certificadas pelo fabricante dos servidores, com a apresentação de uma declaração do mesmo, em como são compatíveis com os servidores existentes. Pretende se o fornecimento das seguintes placas:

- 4 x Placa de rede Low Profile Dual Porto 10Gb/s SFP+ (inclui Transceivers 10Gb SFP+ SR);
- 4 x Placa de fibra Low Profile Dual Porto 16Gb/s;
- 8 x Chicotes de fibra de 7m LC/LC OM4;
- 8 x Chicotes de fibra de 5m LC/LC OM4.

LAN Switch Core

Pretende-se o fornecimento de 2 Switches de rede para interligação dos atuais equipamentos existentes no Município. Cada equipamento deverá cumprir com os seguintes requisitos mínimos:

- Altura Máxima de 1U com guias para fixação em Rack de 19”;
- Mínimo de 48 portos SFP+ 10Gb/s, 2 portos QSFP+ e 4 portos QSFP28;
- 1 Cabo QSFP+ para QSFP+ 40Gbe para interligação dos switches;
- 4 Cabos SFP+ para SFP+ 10Gbe para uplink dos switches de distribuição existentes;
- 8 Transceivers 10Gb SFP+ SR;
- Capacidade de switching mínima de 1.76 Tbps;
- Throughput mínimo de 1320Mpps;
- 1 Porto Consola/Gestão com sinal RS232;

- 1 Porto Consola RJ45 micro-USB-B;
- 1 Porto RJ45 10/100/1000 Base-T para Gestão;
- Fontes de alimentação Hot-Swap e Redudantes;
- Packet buffer memory: 12MB;
- CPU memory: 4GB;
- MAC addresses: 272K (in Scaled L2 mode);
- PVST: 128 instances;
- ARP table 200K (in Scaled L3 host mode);
- IPv4 routes: 200K (in Scaled L3 routes mode);
- IPv6 hosts: 64K;
- IPv6 routes: 130K (in Scaled L3 routes mode);
- Multicast hosts: 8K;
- Link aggregation: 32 links per group, 128 groups;
- Layer 2 VLANs: 4K;
- Layer3 VLANs: 500;
- MSTP: 32 instances;
- LAG load balancing: Based on layer 2, IPv4 or IPv6 headers;
- L2 Ingress ACL: 6K;
- L2 Egress ACL: 1K;
- IPv4 Ingress ACL: 6K;
- IPv4 Egress ACL: 1K;
- IPv6 Ingress ACL: 3K;
- IPv6 Egress ACL: 500;
- IEEE Compliance;
- 802.1AB LLDP;
- TIA-1057 LLDP-MED;
- 802.1s MSTP;
- 802.1w RSTP;
- 802.3ab Gigabit Ethernet (1000Base-T);

- 802.3ad Link Aggregation with LACP;
- 802.3ae 10 Gigabit Ethernet (10GBase-X);
- 802.3ba 40 Gigabit Ethernet (40GBase-X);
- 802.3i Ethernet (10Base-T);
- 802.3u Fast Ethernet (100Base-TX);
- 802.3z Gigabit Ethernet (1000BaseX);
- 802.1D Bridging, STP;
- 802.1p L2 Prioritization;
- 802.1Q VLAN Tagging, GVRP;
- 802.1Qbb PFC;
- 802.1Qaz ETS;
- 802.1s MSTP;
- 802.1w RSTP;
- PVST+;
- 802.1X Network Access Control;
- 802.3ab Gigabit Ethernet (1000BASE-T) or breakout
- 802.3ac Frame Extensions for VLAN Tagging;
- 802.3ad Link Aggregation with LACP;
- 802.3ae 10 Gigabit Ethernet (10GBase-X);
- 802.3ba 40 Gigabit Ethernet (40GBase-SR4, 40GBase-CR4, 40GBase-LR4, 100GBase-SR10, 100GBase-LR4, 100GBase-ER4) on optical ports;
- 802.3bj 100 Gigabit Ethernet;
- 802.3u Fast Ethernet (100Base-TX) on mgmt. ports;
- 802.3x Flow Control;
- 802.3z Gigabit Ethernet (1000Base-X) with QSA;
- ANSI/TIA-1057 LLDP-MED;
- Jumbo MTU support 9,416 bytes;
- 802.1D Compatible;
- 802.1p L2 Prioritization;

- 802.1Q VLAN Tagging;
- 802.1s MSTP;
- 802.1w RSTP;
- 802.1t RVPST+;
- 802.3ad Link Aggregation with LACP;
- VLT Enhancements;
- Minloss Upgrades;
- VLT Proxy Gateway;
- RVPST over VLT;
- DCB, FSB, iSCSI over VLT;
- RSPAN over VLT.

Suporte e Manutenção:

O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado diretamente pelo fabricante com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção pretendida é a seguinte:

Manutenção de 36 meses incluído peças e mão-de-obra:

- SLA 24x7 com tempo de resposta nas instalações do Município no dia útil seguinte
- Prestação de assistência contínua até à solução da avaria.
- O suporte deverá ser dado diretamente pelo fabricante localmente

LAN Switch Distribuição

Pretende-se o fornecimento de 6 Switches de rede para interligação dos atuais equipamentos existentes no Município. Cada equipamento deverá cumprir com os seguintes requisitos mínimos:

- Altura Máxima de 1U com guias para fixação em Rack de 19"
- Mínimo de 48 portos 1Gb/s Base-T, 4 portos SFP e 2 portos SFP+
- 2 Transceivers 10Gb SFP+ SR
- Capacidade de switching mínima de 184 Gb/s
- Throughput mínimo de 131Mpps

Suporte e Manutenção:

O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado diretamente pelo fabricante com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção pretendida é a seguinte:

Manutenção de 36 meses incluído peças e mão-de-obra:

- SLA 24x7 com tempo de resposta nas instalações do Município no dia útil seguinte;
- Prestação de assistência contínua até à solução da avaria;
- O suporte deverá ser dado diretamente pelo fabricante localmente;

SAN Switch:

Pretende-se o fornecimento de 2 Switches SAN de Fibra para interligação dos atuais equipamentos SAN existentes no Município. Cada equipamento deverá cumprir com os seguintes requisitos mínimos:

- Mínimo de 12 portas FC 16Gb/s licenciadas e com respetivos transceivers com possibilidade de crescimento até 24 Portos com a simples adição de licença e transceivers;
- Os portos deveram suportar os seguintes modos de funcionamento: D_Port, E_Port, F_Port, M_Port;
- Frame Buffers mínimos de 8 192 por grupo de 24 Portos, dinamicamente alocados;
- Performance mínima de 8.50Gb/s em Full Duplex a 16Gb/s;
- Largura de banda mínima de 384Gb/s end-to-end full duplex;
- Suporte para duas fontes de alimentação Hot-Swap, redundantes, sendo preciso o fornecimento de apenas uma fonte de alimentação;
- Máximo de 1U de altura, com guias para colocação em Rack de 19”.

Suporte e Manutenção:

O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado diretamente pelo fabricante com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção pretendida é a seguinte:

Manutenção de 36 meses incluído peças e mão-de-obra:

- SLA 24x7 com tempo de resposta nas instalações do Município no dia útil seguinte;
- Prestação de assistência contínua até à solução da avaria;
- O suporte deverá ser dado diretamente pelo fabricante localmente (preferencialmente em língua portuguesa) sem recorrer a qualquer parceiro para esse efeito.

Firewall:

Pretende-se o fornecimento de duas firewalls para funcionamento em Alta Disponibilidade que incorpora uma plataforma de gestão capaz de gerir e monitorizar outros equipamentos instalados local ou geograficamente dispersos. Toda a componente de reporting da solução a adquirir no âmbito deste procedimento deverá ser parte integrante da solução. Cada equipamento a propor deverá cumprir os seguintes requisitos:

- O fabricante deverá ter no mínimo 20 anos de experiência no mercado da segurança, e desenvolver em exclusivo, apenas soluções de segurança;
- O fabricante deverá comprovar a sua liderança em soluções de segurança (UTM, Firewall e prevenção de intrusões) ano após ano, em análises/relatórios de entidades independentes;
- O fabricante deverá endereçar todos os requisitos de um equipamento de segurança (Firewall), tais como processamento de largura de banda, número de ligações, capacidade de garantir a securização de aplicações de nova geração em todas as vertentes da rede (escritório, centro de dados) num único equipamento;
- O fabricante deverá disponibilizar as mesmas funcionalidades de inspeção avançada (Firewall, intrusion prevention, application control, URL filtering, Anti-Bot, Anti-Virus, Sandboxing) em modelo físico e virtual, quaisquer destas geridas por uma única consola central e dedicada;

- A solução proposta, deverá endereçar todas as funcionalidades que se seguem, de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante (single vendor):
 - ✓ Statefull Inspection Firewall - A gateway deverá inspecionar end-to-end (não apenas “half-way” ou “header”) todos os fluxos de comunicação desde o estabelecimento da sessão (3-way handshake TCP), durante a transferência de informação (payload), até que esta seja terminada;
 - ✓ Intrusion Prevention System;
 - ✓ User Identity Acquisition;
 - ✓ Application Control and URL filtering;
 - ✓ Anti – Bot / Anti – Virus;
 - ✓ Threat Emulation (Sandboxing);
 - ✓ Threat Extraction (scrubbing);
 - ✓ Anti – Spam and Email Security;
 - ✓ IPSec VPN;
 - ✓ Remote Access VPN (Mobile Access);
 - ✓ Data Loss Prevention;
 - ✓ Logging and Status;
 - ✓ Event Correlation and Reporting.
- A solução proposta, não poderá em momento algum “sacrificar” a segurança em detrimento da performance (desabilitar inspeção end-to-end em cenários de “carga” na plataforma);
- A solução proposta deverá conter uma plataforma de gestão dedicada com:
 - ✓ Centralização de políticas, logs, reports;
 - ✓ Sem limite de storage com base em requisitos de licenciamento;
 - ✓ O servidor de gestão deverá ter a capacidade de obter detalhes de configuração diretamente das gateways de firewall (fetch de informação de routing, interfaces, etc.) de forma “automática”, e não apenas se estas forem instanciadas previamente via template, a partir do servidor de gestão.
- Requisitos mínimos de Performance:
 - ✓ Threat Prevention/Extraction ≥ 1.7 Gbps;
 - ✓ NextGen Firewall ≥ 3.7 Gbps;

- ✓ Intrusion Prevention System ≥ 4.6 Gbps;
- ✓ VPN Throughput ≥ 2.5 Gbps;
- ✓ Firewall Throughput ≥ 8.5 Gbps;
- ✓ Connections per second 67 k;
- ✓ Concurrent Connections 2 M.
- Requisitos físicos mínimos:
 - ✓ Disco de 240Gb;
 - ✓ 8GB de Memória;
 - ✓ 10 Interfaces 10/100/100;
 - ✓ 1Modulo de 4x 10Gb SFP+ com respetivos Transceivers;
 - ✓ Interface de Gestão dedicado;
 - ✓ Interface HA.
- Possibilidade de expandir a memória até 32 GB;
- Modularidade de interfaces:
 - ✓ Deverá ser flexível quanto o número/tipos de interfaces a aplicar ao chassis:
 - 8x1GE UTP (até 18 portas);
 - 4x1GE SFP (até 4 Portas);
 - 4x10GE SFP+ (até 4 Portas).
- Possibilidade de Interface LOM (Lights Out Management);
- Possibilidade de Fontes de Alimentação Redundantes;
- Dimensões: 438 x 508 x 44mm;
- Peso: 6.75/7.5 kg.

Requisitos - Funcionalidades de rede:

- Suporte para 1024 interfaces vlan;
- Suporte para 4096 interfaces vlan (em cenário de contextos virtuais de firewall);
- Suporte para protocolos de agregação de links (LACP 802.3ad);
- Suporte para funcionamento em modo L2 (bridging) e L3 (routing);
- Suporte de NAT;
 - ✓ Static, Hide, PAT;

- ✓ NAT44, NAT46, NAT64, NAT66.
- Suporte para routing estático;
- Suporte para Policy Based Routing (PBR);
- Suporte para protocolos de routing dinâmico:
 - ✓ BGP, OSPF (v2 | v3), RIP;
 - ✓ Suporte para multicast.
- Routing Multicast;
 - ✓ L2 (IGMP v1 | v2);
 - ✓ L3 (PIM-SM, PIM-SSM, PIM-DM).

Requisitos de alta disponibilidade:

- Activo/Passivo ou Activo/Standby
 - ✓ VRRP ou IP Virtual;
 - ✓ Failover:
- Falhas de routing;
- Falhas de dispositivo;
- Falhas de link;
 - ✓ Sincronização de sessões entre membros do cluster.

Requisitos técnicos/lógicos:

- O equipamento de segurança, deve utilizar a tecnologia de Stateful Inspection, para construir e manter a tabela de sessões (fluxos de comunicação);
- O Equipamento de segurança deve ser capaz de suportar o debito, número de novas ligações e manutenção das mesmas de acordo com as necessidades do cliente;
- A solução deve identificar/controlar o acesso de pelo menos 150 serviços/protocolos;
- Na interface da plataforma de gestão deve ser possível visualizar número de acessos por regra;
- A solução tem de suportar que se apliquem regras em intervalos de tempo, para que seja possível definir o tempo útil das mesmas;
- A comunicação entre a firewall e a solução de gestão, tem de ser encriptada e autenticada com recurso a infraestrutura própria de PKI;

- A Firewall tem de suportar métodos de autenticação por sessão, utilizadores e clientes;
- Os seguintes métodos de autenticação de utilizadores têm de ser suportados pelos módulos de VPN e Firewall:
 - ✓ Tokens (ie -SecureID);
 - ✓ TACACS;
 - ✓ RADIUS;
 - ✓ Certificados Digitais.
- A solução tem de ter base de dados de utilizadores local, para permitir a autenticação e autorização dos mesmos sem recurso a um dispositivo externo;
- A solução tem de suportar as funções de DHCP server e Relay;
- A solução tem de suportar o suportar a função de proxy em HTTP e HTTPS;
- A solução tem de ter capacidade de trabalhar em modo transparente/Bridge (L2);
- A solução tem de suportar alta disponibilidade ou load-sharing e sincronização de estados entre os dois membros do cluster.

Sistema de prevenção de intrusões (IPS):

- O fabricante deve fornecer evidências da sua posição de liderança, ano após ano, no Quadrante Mágico do Gartner para:
 - ✓ Soluções de Prevenção de Intrusão;
 - ✓ Soluções de Firewall Enterprise.
- O IPS deve ser baseado nos seguintes mecanismos de deteção:
 - ✓ Assinaturas;
 - ✓ Anomalias no protocolo;
 - ✓ Controlo Aplicacional;
 - ✓ Análise de comportamento.
- Os Módulos de IPS e firewall devem estar integrados na mesma plataforma;
- O administrador deve ter a possibilidade de configurar a inspeção para proteção apenas da rede interna;
- O IPS deve ter opções para criar perfis com base em assinaturas para proteção de Clientes ou servidores. Também deve ser possível criar um perfil para proteção de ambos;

- O IPS deve fornecer pelo menos dois perfis/políticas predefinidas que podem ser utilizados no deployment da solução;
- O IPS deve ter um mecanismo fail-open baseado em software, ajustável com base em limites do gateway, CPU ou utilização de memória;
- O IPS deve ter mecanismo automático para ativar ou gerir as novas assinaturas após atualizações;
- O IPS deve suportar exceções com base em origem, destino, protocolo, ou uma combinação dos três;
- O IPS deve permitir mudar para o modo de deteção, sem alterar parâmetros individuais, por forma a facilitar as ações de troubleshooting;
- O IPS deve possuir uma solução centralizada de correlação e relatório de eventos;
- O administrador deve poder ativar de forma automática novas proteções, com base em parâmetros configuráveis:
 - ✓ impacto no desempenho;
 - ✓ Grau de severidade da ameaça;
 - ✓ nível de confiança;
 - ✓ proteções do cliente;
 - ✓ proteções do servidor.
- O IPS deve ser capaz de detetar e prevenir os seguintes tipos de ameaça:
 - ✓ uso indevido de protocolo;
 - ✓ comunicações de malware;
 - ✓ tentativas de uso de protocolos de tunneling;
 - ✓ tipos genéricos de ataque sem assinaturas predefinidas.
- Para cada proteção, a solução deve incluir o tipo de proteção (relativamente a servidor ou cliente):
 - ✓ gravidade da ameaça;
 - ✓ impacto no desempenho;
 - ✓ nível de confiança;
 - ✓ referência - (ie CVE).
- O IPS deve ser capaz de capturar pacotes/evidencias para proteções específicas;

- O IPS deve ser capaz de detetar e bloquear ataques nas layers de network e application layer, protegendo pelo menos os seguintes tipos de serviços:
 - ✓ Serviços de email;
 - ✓ DNS;
 - ✓ FTP;
 - ✓ Serviços do Windows (Microsoft Networking).
- O fornecedor deve fornecer evidências de liderança na proteção de vulnerabilidades Microsoft;
- O IPS e/ou o Application Control deve incluir a capacidade de detetar e bloquear aplicações P2P e evasivas (Anonymizers);
- O administrador deve poder definir exclusões a plataforma de IPS, baseadas em redes ou hosts;
- A solução deve proteger DNS Cache Poisoning e impedir o acesso dos utilizadores a endereços de domínio bloqueados;
- Solução deve fornecer proteções para protocolos VOIP;
- O IPS e/ou o Application Control devem detetar e bloquear aplicações que permitam controlo remotos, incluindo as que são capazes de realizar tunneling sobre o tráfego HTTP
- IPS deve ter proteções SCADA;
- IPS deve possibilitar a conversão de assinaturas SNORT;
- A solução deve permitir ao administrador bloquear de forma fácil o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os intervalos de IP correspondentes ao país.

Aquisição de identidade de utilizadores (User ID Acquisition):

- Deve ser capaz de adquirir a identidade dos utilizadores, com base na consulta dos eventos de segurança da Microsoft Active Directory;
- Deve ser possível a autenticação através de uma browser, numa base de dados local, para utilizadores ou dispositivos que não pertençam ao domínio;
- Deve ter um agente que possa ser instalado nos endpoints, para reportar a firewall as identidades dos utilizadores;

- A solução deve integrar-se perfeitamente com Microsoft Active Directory, IF-MAP e Radius;
- O impacto do uso da solução de aquisição de identidade no CPU das AD, deve ser inferior a 3%;
- A solução de aquisição de identidade deve suportar soluções de Terminal server e citrix;
- A solução deve permitir a identificação de utilizadores que acedem através de um proxy (exemplo: X-forwarded headers);
- Deve ser capaz de adquirir a identidade de um utilizador presente numa Microsoft Active Directory sem qualquer tipo de agente instalado no controlador de domínio;
- Deve suportar autenticação Kerberos para single sign on;
- Deve suportar LDAP nested groups;
- Deve ser capaz de partilhar identidades de utilizadores entre vários gateways de segurança;
- Deve ser capaz de criar identity roles (grupos de identidades) para serem invocados em diferentes aplicações da solução.

Filtragem de URL e Controlo de Aplicações:

- A solução deve reconhecer e controlar mais de 8000 aplicações conhecidas;
- A base de dados da solução deve conter mais de 200 milhões de URL's categorizados, abrangendo mais de 85% da Alexa's top 1M sites;
- A solução deve permitir criar uma regra de filtragem de conteúdos com várias categorias;
- A solução deve permitir filtrar conteúdos de URL's baseada em HTTPS sem efetuar inspeção de SSL;
- A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias;
- A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores;
- A solução, após 4 semanas de produção, deve ter em cache cerca de 99% das solicitações de categorização;
- A solução deve ter uma interface fácil de pesquisa de aplicações e URL's;
- A solução deve categorizar aplicações e URL's por fator de risco;
- A política de URLF e Application Control deve poder ser definida por identidade do utilizador;

- A base de dados de URLF e Application Control devem ser atualizados por um serviço Cloud;
- A solução deve ter o controlo de aplicações e URLF unificado na mesma política;
- A solução deve ter mecanismos para informar ou perguntar ao utilizador em tempo real, para os educar ou para confirmarem as suas ações com base na política de segurança;
- A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda;
- A solução deve permitir exceções com base em objetos de rede previamente definidos;
- A solução deve fornecer a opção de modificar a página de Bloqueio e redirecionar o utilizador para uma página de remediação;
- A solução deve incluir um mecanismo de Black e White List, para permitir que se negue ou permita URL's específicos, independentemente da categoria;
- A solução deve fornecer um mecanismo de substituição na categorização de URL.

Anti-bot e Anti-Virus:

- O fornecedor deve ter solução de Anti-Bot e Anti-Virus integrado na firewall;
- A Solução de Anti-Bot deve ser capaz de detetar e parar comportamentos de rede suspeitos;
- O aplicativo Anti-Bot deve usar um mecanismo de deteção baseado em vários pontos, reputação de endereços IP, URLs e DNS e detectar padrões de comunicação de bots;
- A proteção Anti-Bot deve ter capacidade de efetuar Scan a ações de bot;
- A solução deve apoiar a detecção e prevenção de vírus e variantes de Cryptors & ransomware (por exemplo, Wannacry, Cryptlocker, CryptoWall ...) através do uso de análise estática e/ou dinâmica;
- A solução deve ter suporte para proteção contra-ataques de spear phishing;
- DNS based attacks - A solução deve ter recursos de detecção e prevenção para C&C DNS hideouts:
 - ✓ Pesquisa de padrões de tráfego de C & C, não apenas no destino de DNS;
 - ✓ Reverse engineer do Malware para descobrir seu DGA (Domain Name Generation);
 - ✓ DNS Trap, como parte da política de ameaças, interceta e analisa tentativas de comunicações do endpoint com C&C;
 - ✓ A solução deve detetar e prevenir ataques de DNS tunneling.

- A política de Anti-Bot e Anti-Virus deve ser gerida a partir de uma consola central;
- A solução de Anti-Bot e Anti-Virus deve ter um mecanismo centralizado de correlação e relatório de eventos;
- A solução de antivírus deve ser capaz de impedir o acesso a sites maliciosos;
- A solução de antivírus deve poder inspecionar o tráfego SSL;
- O Anti-Bot e o Anti-Virus devem ter atualizações em tempo real na cloud;
- O Antivírus deve ser capaz de impedir a entrada de arquivos maliciosos;
- O Antivírus deve ser capaz de analisar arquivos compactados;
- Políticas antivírus e Anti-Bot devem ser geridas centralmente e ser possível a parametrização das mesmas;
- O Antivírus deve suportar a análise de links dentro de emails;
- O antivírus deve analisar os ficheiros que estão a passar no protocolo CIFS.

Emulação e Extração de Ameaças:

- A solução deve ter a capacidade de proteger contra os ataques desconhecidos (malware Zero Day) antes que proteções de assinatura estática sejam criadas:
 - ✓ Proteção em Tempo Real para malware desconhecido na navegação Web;
 - ✓ Proteção em Tempo Real para malware desconhecido em email.
- Cenários de implantação:
 - ✓ A solução deve fazer parte da arquitetura de prevenção de ameaças (com IPS, AV, AB, URLF, APP FW);
 - ✓ A solução deve fornecer solução de implementação On Prem e Cloud Based;
 - ✓ Solução de Cloud pura;
 - ✓ A solução deve suportar integração com 3rd party (public API);
 - ✓ A solução deve suportar implementação em modo in-line;
 - ✓ A solução deve suportar a implementação modo MTA (Mail Transfer Agent);
 - ✓ A solução deve suportar implementação em modo de porta TAP / SPAN;
 - ✓ A solução não deve exigir infraestrutura separada para proteção email e proteção Web;
 - ✓ A solução deve suportar a implementação em modo cluster.

- Tipos de ficheiros Suportados - A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash especificamente:
 - ✓ 7z, cab, csv, doc, docm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsx, xlt, xltm, xltx, xlw, zip, pif, com, gz, bz2, tgz, apk(android), ipa (iphone), ISO, js, cpl, vbs, jse, vba, vbe, wsf, wsh;
- A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash, que sejam transmitidos pelos protocolos:
 - ✓ HTTP;
 - ✓ HTTPS;
 - ✓ FTP;
 - ✓ SMTP;
 - ✓ CIFS (SMB);
 - ✓ TLS SMTP;
- OS support:
 - ✓ O mecanismo de emulação deve suportar vários sistemas operativos, como XP e Windows7, 8,10 32/64 bits, incluindo imagens personalizadas;
 - ✓ A solução deve suportar cópias LICENCIADAS de Microsoft WINDOWS e Microsoft Office através de um contrato com a Microsoft;
 - ✓ A solução deve detectar chamadas API, alterações em ficheiros, system registry, ligações de rede e processos do sistema;
 - ✓ A solução deve suportar análise estática para windows, mac OS-X, Linux ou qualquer plataforma x86;
- O mecanismo de emulação deve ser capaz de inspecionar, emular, prevenir e compartilhar os resultados do evento de sandbox na infraestrutura de anti-malware;
- A solução deve permitir a emulação de ficheiros maiores que 10 Mb, em todos os tipos suportados;
- A solução deve suportar automated machine learning based detection engines;
- A solução deve detectar o ataque na fase de exploitation - ou seja, antes que o código seja executado e antes que se tenha concluído o download do malware;

- A solução deve detectar ROP e outras técnicas de exploitation (por exemplo, elevação de privilégios), analisando o CPU;
- A solução deve suportar a análise de links no corpo do e-mail para deteção de Malware Zero Day;
- A solução deve ser capaz de verificar o histórico de URLs registrados nos últimos X e-mails e verificar se a classificação foi alterada (por exemplo: de Clean para malicious);
- Tempo médio de emulação, para um veredito de malware suspeito como benigno não deve ser muito superior a 1 minuto;
- Tempo médio de emulação, para um veredito de malware suspeito como maligno não deve ser muito superior a 3 minutos;
- A solução de emulação de ameaças deve permitir "Geo Restriction", que permite que as emulações sejam restritas a um país;
- A solução deve possuir um mecanismo automático de partilha de informação com outros gateways em meio a atualizações de assinaturas etc, por forma a partilhar informações sobre novos ataques;
- O mecanismo de emulação deve exceder 90% na taxa de captura nos testes do Total de vírus em que os PDFs e os arquivos maliciosos conhecidos são modificados com cabeçalhos "não usados" para demonstrar a capacidade das soluções de detetar malwares desconhecidos;
- A solução deve detetar o tráfego de C & C de acordo com a reputação dinâmica de ip / url;
- A solução deve ser capaz de emular e extrair arquivos incorporados em documentos;
- A solução deve ser capaz de analisar documentos com URL's;
- Na funcionalidade de Sandboxing/Scrubbing, a solução proposta deverá ter a capacidade de suportar deteção de ameaças e técnicas de evasão (com tentativas de explorar vulnerabilidades de S.O.) ao nível do CPU – CPU-Level detection.

Deteção de atividades em sistema:

- A solução deve ter a capacidade de detetar atividades fora de “padrão de utilização/protocolo”:
 - ✓ Chamadas de API;
 - ✓ Alterações no sistema de arquivos;

- ✓ Alterações de Registo;
- ✓ Ligações de rede;
- ✓ Em Processos do sistema Operativo;
- ✓ Criar e eliminar arquivos;
- ✓ Modificação de arquivos;
- ✓ Adição de código ao kernel;
- ✓ Detetar tentativas de elevação de privilégios;
- ✓ Alterações no kernel (Alterações de memória realizadas pelo código do kernel, não o fato de que um driver ser carregado - isso é controlado pelo item acima);
- ✓ Análise de comportamento do kernel (analisar a atividade do código, não as alterações efetuadas pelo utilizador);
- ✓ Contornar UAC (user access control);

Mecanismos Anti-evasão:

- A solução proposta deverá ter capacidade de deteção de técnicas de evasão (emulação/sandboxing) para posterior reação e mitigação de ameaças;
- A solução deverá ser resiliente e identificar casos onde a execução de código malicioso (malware/shell-code) não ocorra mediante a deteção de um ambiente virtualizado (técnica de evasão para contornar mecanismos de deteção por sandboxing);
- A solução deverá ser resiliente e detetar delays implementados na execução de código malicioso (malware/shell-code);
- A solução deverá ser resiliente a situações em que a execução de código malicioso (malware/shell-code) apenas ocorre após um restart/shutdown da workstation/endpoint infetado.

Extração de ameaças (File Scrubbing/Flattening):

- A solução proposta deverá ter a capacidade de eliminar ameaças existentes em conteúdos dinâmicos/objetos embebidos em ficheiros;
- A solução proposta deverá ter a capacidade de reconstrução dos ficheiros, excluindo os conteúdos ativos, e mantendo apenas conteúdos seguros;

- A solução proposta deverá ter a capacidade de converter ficheiros reconstruídos (em que os conteúdos ativos foram excluídos) em formato PDF, para serem entregues em tempo real ao utilizador, de forma a melhorar a experiência de utilização;
- A solução proposta deverá ser configurável e flexível, de forma a possibilitar manter o formato do ficheiro original, especificando o tipo de conteúdo a ser removido.

Anti-Spam & Email Security:

- A solução deverá ser agnóstica em relação ao conteúdo, e ter a capacidade de classificar ameaças em tempo real, protegendo a infraestrutura com base padrões comportamentais, e não com base em conteúdo;
- A solução proposta deverá incluir mecanismos de proteção com base em serviços online de IP reputation, de forma a evitar falsos positivos;
- A solução deverá incluir mecanismos de proteção imediata (Dia Zero) para novos vírus propagados por email.

IPsec VPN:

- A solução deverá suportar implementações de VPN (domain based, e route based com protocolos de routing dinâmico e virtual tunnel interfaces), com utilização de Internal Certificate Authority ou External 3rd party Certificate Authority;
- A solução deverá suportar criptografia 3DES e AES-256 para IKE Phase 1 e 2;
- A solução deverá suportar criptografia IKEv2 plus "Suite-B-GCM-128" e "Suite-B-GCM-256" for IKE Phase 2;
- A solução deverá suportar os seguintes grupos Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20;
- A solução deverá suportar os seguintes tipos de mecanismos de integridade de dados: md5, sha1, SHA-256, SHA-384 and AES-XCBC;
- A solução proposta deverá suportar as seguintes funcionalidades VPN:
 - ✓ Site-to-site:
 - Full Mesh (todos para todos);
 - Estrela (Sites remotos para Site principal);
 - Hub&Spoke (Site remotoA para Site RemotoB, através de site principal);

- Suporte para configuração através de GUI, com opção de drag&drop de objetos nas comunidades VPN.
- ✓ Suporte para VPN's de acesso remoto "clientless" e "client based";
- ✓ Suporte para aplicação de políticas de segurança específicas, para controlo de tráfego associado à comunidade VPN;
- ✓ A solução proposta deverá incluir licenciamento para 50 VPN's simultâneas.

Security Management:

- A solução deverá possibilitar a segmentação da política de segurança numa estrutura de subpolíticas;
- A solução deverá possibilitar a segmentação da política de segurança numa estrutura de layers;
- A solução deverá possibilitar a integração de logs e audit logs numa única consola, para contextualizar o administrador ao efetuar alterações sobre a política de segurança;
- A solução de gestão deverá suportar role based access control, para segregar acessos de administração para gestão de política e visualização de logs;
- A solução deverá implementar um mecanismo de comunicação segura, assente em certificados, entre todas as componentes de segurança integradas no sistema de gestão centralizada;
- A solução deverá incluir um Certificate Authority x.509 com capacidade para gerir/gerar certificados internos, para autenticação de utilizadores em acessos VPN remotos;
- A solução deverá disponibilizar um mecanismo de pesquisa para facilitar a utilização e identificação de objetos, com base no seu endereço IP;
- A solução deverá disponibilizar métricas de "hit count" nas regras presentes na política de segurança;
- A solução deverá possibilitar a utilização de etiquetas (labels) ou secções (tabs) para melhor organização da política de segurança;
- A solução deverá permitir gravar a política de forma integral ou parcial;
- A solução deverá disponibilizar um mecanismo de validação da política de segurança, antes da sua instalação nas gateways de firewall;

- A solução deverá disponibilizar um mecanismo de backup e revisão da política de segurança, possibilitando comparar versões da política e reverter para versões anteriores, se necessário.

Logging e Monitorização:

- A solução de logging, deverá estar integrada na componente de gestão centralizada, e possibilitar a visualização de logs afetos a políticas específicas, sem ser necessário recorrer a uma nova janela, ou aplicação;
- A solução deverá poder ser integrada na componente de gestão centralizada, ou numa appliance/máquina virtual dedicada;
- A solução deverá ter a capacidade de produzir logs de todas as políticas (30k logs/seg);
- A solução deverá ter a capacidade de consolidar os logs de todas as componentes de segurança que se encontrem ativas na plataforma: IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, User Identity, Mobile Access;
- A solução deverá suportar um mecanismo de captura de pacotes para eventos de IPS, para facilitar despiste e análise forense;
- A solução deverá implementar um mecanismo seguro de forwarding de logs, com autenticação e encriptação, para evitar potenciais ataques (ex. Eavesdropping):
 - ✓ Os logs deverão ser transferidos de forma segura entre a FW gateway, o log server, e o utilizador final.
- A solução deverá disponibilizar detalhes sobre o estado de todos os túneis IPSEC, site-to-site e remote access (client-to-site);
- A solução deverá possibilitar a customização de valores de threshold, para execução de ações, uma vez atingido/ultrapassado esse threshold: log, alert, snmp-trap, email notification;

Correlação de eventos e reporting:

- A solução deverá integrar a componente de reporting e correlação de eventos com a sua componente de gestão centralizada;
- A solução deverá ter a capacidade de correlacionar eventos de todas as funcionalidades ativas nas demais gateways (FW, IPS, URL-F, etc.);

- A solução deverá possibilitar a criação de filtros de logging, com base em qualquer característica, tal como: aplicação, ip de origem e destino, serviço, tipo de evento, severidade do ataque, país de origem e destino, etc.;
- A solução deverá disponibilizar um mecanismo para assignar os filtros criados a diferentes tipos de gráficos, a serem atualizados periodicamente, apresentando todos os eventos que igualem o filtro aplicado, permitindo ao operador focar-se nos eventos mais importantes;
- A solução deverá assegurar a possibilidade de pesquisar na lista de eventos, e garantir o “drill down” de detalhes em pesquisas e análise forense;
- A solução deverá ter capacidade de detetar e alertar para eventos de login de administradores, em horários não frequentes;
- A solução deverá detetar ataques de “credential guessing / brute force”;
- A solução deverá reportar todos os eventos de alteração/instalação de políticas de segurança;
- A solução deverá incluir relatórios horários, diários, semanais e mensais predefinidos, incluindo pelo menos: Top Events, Top Sources, Top Destinations, Top Services, etc.;
- A solução de reporting deverá disponibilizar informação consolidada sobre:
 - ✓ Volume de ligações bloqueadas por uma regra de segurança em particular;
 - ✓ Top de origens bloqueadas, e os destinos e serviços respetivos;
 - ✓ Top de regras mais utilizadas na política de segurança;
 - ✓ Top de ataques detetados no perímetro, com informação das origens e destinos associados;
 - ✓ Atividade web por user, com top de web users e websites mais utilizados.

Compliance e Boas Práticas:

- A solução deverá contemplar Risk Governance e Compliance totalmente integrado na componente de gestão centralizada;
- A solução deverá ter uma opção para controlar o cumprimento em tempo real de todos os serviços de segurança do produto;
- A solução deverá ter uma opção para entregar a avaliação em tempo real de acordo com as regulamentações principais (tais como: PCI-DSS, HIPAA, SOX, GDPR...);

- A solução deverá ter uma opção para notificação imediata sobre as mudanças nas políticas que afetem o cumprimento das certificações;
- A solução deverá ter uma opção para disponibilizar recomendações práticas para melhorar a conformidade de segurança;
- A solução deverá ter uma opção para recomendar Práticas recomendadas de segurança;
- A solução deverá ter uma opção para traduzir os requisitos regulamentares em melhores práticas de segurança acionáveis;
- A solução deverá ter uma opção para monitorizar constantemente a configuração das gateways com as melhores práticas de segurança;
- A solução deverá ter uma opção para gerar relatórios de avaliação automatizados para avaliar a conformidade com os principais regulamentos;
- A solução deverá ter uma opção para integrar plenamente na infraestrutura de arquitetura de Software e Gestão;
- A solução deverá ter uma opção para verificar a conformidade com cada mudança de política para todas as funcionalidades dos equipamentos de firewall.

SSL Inspection (inbound / outbound):

- A solução deverá suportar inspeção SSL (inspection/decryption) com performance comprovada em todas as tecnologias de mitigação;
- A solução deverá suportar Perfect Forward Secrecy (PFS , ECDHE cipher suites);
- A solução deverá suportar AES-NI, AES-GCM for improved throughput;
- A solução deverá suportar a integração das tecnologias de emulação/sandboxing com inspeção SSL;
- A solução deverá permitir a reutilização da base de dados de URL Filtering, para criação de políticas de inspeção de SSL granulares.

Suporte e Manutenção:

O suporte e manutenção, deve ser assegurado diretamente pelo fabricante.

A manutenção pretendida é a seguinte:

Manutenção de 12 meses incluído peças e mão-de-obra:

- SLA 24x7 com tempo de resposta nas instalações do Município no dia útil seguinte
- Prestação de assistência contínua até à solução da avaria.

Solução Scale-out NAS:

Pretende-se implementar uma solução robusta e escalável, suportada numa arquitetura scale-out para o rápido crescimento e a melhor partilha de recursos em termos de infraestrutura. A solução a propor deverá cumprir com os seguintes requisitos:

- Solução All-Flash. Não serão aceites soluções baseadas em equipamentos híbridos configurados apenas com discos SSD;
- Disponibilizar 7 TiB úteis, sem recorrer a qualquer mecanismo de eficiência, considerando uma tolerância à falha mínima de 2 discos em qualquer posição ou 1 nó qualquer completo e 1 disco em qualquer posição;
- Disponibilizar um mínimo de 3 Nós/controladores;
- Capacidade de ligação de front-end mínima de 50 Gbits por controlador;
- Mínimo de 48 GB de cache por nó/controlador;
- Contemplar a capacidade de balancear utilizadores, estabelecer quotas, snapshots, replicação remota, HDFS e Swift e elaborar reporting sobre a plataforma;
- Rede interna (back-end) redundante de alto débito, com capacidade de ligação mínima de 50 Gbits por controlador.

O sistema tem ainda que suportar os seguintes requisitos:

- Capacidade de disponibilizar um único filesystem superior a 20 PBytes;
- Capacidade de escalar, no mínimo, a 250 nós/controladoras;
- Capacidade de balanceamento de utilizadores pelos diversos controladores através de DNS;
- Integração autenticação Active Directory, Users/grupos locais, LDAP;
- Capacidade de integrar múltiplas Active Directories ou múltiplas fontes de autenticação;

- Capacidade de sincronismo entre sistemas de armazenamento, assim como definir qualidade de serviço e portas físicas pelo qual se replicam os dados;
- Capacidade monitorização do sistema, chargeback, taxas de utilização ao nível dos variados diretórios, comparação entre reporting com deltas entre os mesmos;
- Capacidade de aceleração de metadados em modo leitura/escrita em discos SSD ou memória;
- Capacidade de realizar tiering de dados entre nós/controladores distintos baseado em políticas definidas pelo administrador com possibilidade de alteração do esquema proteção;
- Capacidade de realizar tiering de forma transparente e baseada em políticas para um subsistema de armazenamento Object Storage e para Cloud Pública e Privada;
- Deverá permitir a criação/utilização de múltiplas políticas de tiering em simultâneo;
- Capacidade de utilizar versionamento em simultâneo com as políticas de tiering acima referidas;
- Capacidade aquando de upgrades de nós/controladores, os dados serem balanceados de forma automática para maior utilização de todos os recursos disponíveis;
- Capacidade de definir regras para que sempre que existam upgrades os controladores terem configuradas de forma automática toda a componente de rede;
- O sistema deve ter a capacidade interna de migrar dados sem impactar a rede LAN na troca ou upgrade de controladores;
- Capacidade de dar mais ou menos prioridade a processos a correr no sistema;
- O sistema deve permitir a agregação de portas por controlador;
- Capacidade de alterar a tolerância á falha ao nível do diretório e subdiretório sem implicar migração de volumes entre o sistema;
- Capacidade de replicação local ao nível de um único diretório ou subdiretório dentro de um filesystem;
- Capacidade de upgrades de firmware, controlador a controlador de forma automática sem perda do acesso aos dados em ambientes NFS;
- Capacidade on-demand de alocar ou retirar portas físicas às subnets/redes associadas;
- Upgrade de controladores deverá ser online, de forma simples, com balanceamento de dados automático;

- Capacidade de balanceamento de dados entre controladores para evitar “hot spots” e ter máximo desempenho possível. O balanceamento de dados deverá ser interno sem impactar a rede de produção;
- Capacidade de mapear shares de rede via um único IP podendo com isso chegar a qualquer controlador;
- Integração com ambientes de analítica hadoop, ou seja, capacidade de funcionar como um datanode sendo cada controlador um name node da solução;
- Capacidade de ter múltiplas distribuições de hadoop a aceder aos mesmos dados;
- Suporte de falha até N+4 controladores num único filesystem;
- Suporte de HDFS nativo sem necessidade de qualquer plugin instalado nos servidores de computação;
- Suporte de VLANs;
- Suporte de ICAP para integração com anti-virus;
- Suporte protocolos:
 - ✓ NFS v3, v4;
 - ✓ S3;
 - ✓ SMB1, SMB2, SMB3 e SMB3-CA;
 - ✓ HTTP/HTTPS;
 - ✓ FTP;
 - ✓ REST;
 - ✓ SMTP;
 - ✓ NDMP;
 - ✓ HDFS.

Suporte e Manutenção:

O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado directamente pelo fabricante com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção pretendida é a seguinte:

Manutenção de 36 meses incluído peças e mão-de-obra:

- SLA 24x7 com tempo de resposta nas instalações do Município no dia útil seguinte;

- Prestação de assistência contínua até à solução da avaria;
- O suporte deverá ser dado diretamente pelo fabricante localmente (preferencialmente em língua portuguesa).

Solução Object Storage:

Pretende-se dotar o Município com uma solução flexível e escalável on-prem, que permita uma integração transparente com a plataforma Tier 1 proposta e com a capacidade mínima de 480TB RAW.

Esta solução deverá ter as seguintes características mínimas:

- Deverá estar disponível em 3 formatos diferentes de consumo:
 - ✓ Appliance (incluindo hardware e software);
 - ✓ Apenas software, disponível para ser instalado em commodity hardware;
 - ✓ Cloud pública e/ou privada.
- Deverá crescer através da adição dinâmica de nós:
 - ✓ Deverá permitir nós de gerações diferentes (por exemplo, processadores e diferentes configurações de discos) no mesmo sistema;
 - ✓ A capacidade adicionada deverá estar imediatamente disponível para consumo (independentemente de algum balanceamento de dados interno que possa existir).
- Deverá permitir crescer sem interrupção (online) quando necessário suportando o rebalanceamento automático dos dados por todos os nós/discos adicionados;
- A configuração proposta deverá ser desenhada de modo a que, em caso de falha de um nó, não deverá reduzir mais de 25% a capacidade útil disponível;
- A plataforma proposta deverá suportar nativamente (sem recurso a gateways externas) os seguintes protocolos:
 - ✓ AWS S3;
 - ✓ OpenStack Swift;
 - ✓ CAS;
 - ✓ NFS;
 - ✓ HDFS.

- Deverá ter mecanismos de paralelismo de escrita para otimização de uploads;
- Deverá permitir ingerir dados através de protocolos de objecto e disponibiliza-los através de protocolos de ficheiro (incluindo HDFS) e vice-versa;
- Deverá suportar OpenStack Keystone v3 na API OpenStack Swift;
- Deverá suportar a retenção de dados para toda a capacidade do sistema de objetos, garantindo a imutabilidade dos mesmos, de acordo com a norma SEC 17a4(f);
- Deverá permitir definir tempos de retenção para diferentes categorias de objetos/conteúdos no caso da(s) aplicação(ões) não o suportarem;
- Deverá permitir a criação de regras de expiração, que permitam a remoção automática dos dados expirados sem intervenção adicional do utilizador e/ou da aplicação;
- Deverá permitir alterar o período de retenção baseado em eventos (por ex. permitir a expiração 10 anos depois de um processo em tribunal ter terminado);
- Deverá proteger todos os objetos através de Erasure Coding;
- Os dados deverão ser protegidos de falhas locais através de erasure coding e de falhas de site completas através de replicação;
- Deverá suportar uma arquitetura dispersa por 2 ou mais sites;
- Deverá disponibilizar o acesso a qualquer objeto através de qualquer um dos nós, em qualquer um dos sites, disponibilizando sempre a versão mais recente dos dados;
- Deverá permitir a pesquisa por metadados;
- Deverá recuperar de qualquer falha a nível de disco ou nó sem dependências de conectividade ao(s) site(s) remoto(s):
 - ✓ Todas as reconstruções de disco e nós deverão apenas consumir recursos no site local, sem consumo de largura de banda WAN;
 - ✓ Em caso de falha de disco ou nó, deverá redistribuir os dados afetados pelo máximo número de nós e discos possíveis, minimizando assim a exposição dos dados à falha ao mesmo tempo que tira partido de um maior número de discos.
- Deverá assegurar o mesmo desempenho para objetos pequenos e grandes;
- Deverá permitir a encriptação Data-at-Rest e In-flight de todos os objetos;
- Deverá permitir a funcionalidade de versionamento das alterações efetuadas a nível do objeto;

- Deverá permitir implementar uma arquitetura multi-tenant, incluindo a capacidade de aplicar limites de quotas em secções específicas do equipamento;
- Deverá disponibilizar REST APIs;
- Deverá garantir uma durabilidade mínima dos dados de 99.999999999% (11 9's).

Suporte e Manutenção:

O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado diretamente pelo fabricante. A manutenção pretendida é a seguinte:

Manutenção de 36 meses incluído peças e mão-de-obra:

- SLA 24x7 com tempo de resposta nas instalações do Município no dia útil seguinte
- Prestação de assistência contínua até à solução da avaria.
- O suporte deverá ser dado diretamente pelo fabricante localmente.

Serviços de Instalação:

Pretende-se o fornecimento dos seguintes serviços:

Upgrade Servidores:

- Instalação das Placas propostas nos servidor Dell EMC PowerEdge R810, R820 e R710;
- Reconfiguração das redes virtuais nos HiperVisores;
- Configuração das Zonas nos SAN Switches para acessos ao storage Dell EMC SC9000 existente;
- Registo das Novas HBA no storage Dell EMC SC9000 para apresentação dos volumes já existentes;
- Testes de funcionamento.

LAN Switch Core e Distribuição:

- Instalação física dos equipamentos em Bastidores;
- Configuração dos equipamentos na rede do cliente;
- Configuração Stack/VLT;

- Configurações LAG, VLAN's, ACL, Uplinks;
- Testes de funcionamento.

SAN Switch:

- Instalação física dos equipamentos em Bastidores;
- Configuração dos equipamentos na rede do cliente;
- Migração das zonas dos SAN Switch existentes para Novos;
- Configuração das Zonas para as novas placas HBA dos servidores Dell EMC existentes;
- Configuração das Zonas de servidor UNISYS ES7000 existente;
- Verificação do acesso dos servidores Dell EMC e UNISYS aos respetivos volumes;
- Testes de funcionamento.

Firewalls:

- Instalação física dos equipamentos em Bastidores;
- Configuração dos equipamentos na rede e domínio do cliente;
- Configuração do cluster FW;
- Ativação de todas as funcionalidades da Firewalles;
- Testes de funcionamento e alta disponibilidade;
- Migração das regras das atuais Firewalls para Novas Firewalls;
- Testes de funcionamento.

Storage NAS:

- Instalação física dos equipamentos em Rack;
- Inicialização do sistema na rede e domínio do cliente;
- Definição do nível de proteção;
- Instalação do último sistema operativo recomendado pelo fabricante;
- Integração com AD;
- Configuração de alertas de e-mail, SNMP conforme necessário;
- Implementação de partilha de CIFS shares, NFS;

- Ativação das funcionalidades de Deduplicação;
- Implementação de políticas de Quotas;
- Configuração de regras de Tiering para o Object Storage proposto;
- Instalação\Configuração de Software de Monitorização;
- Testes de funcionamento;
- Condução de uma transferência de conhecimento.

Object Storage:

- Instalação física dos equipamentos em Rack;
- Inicialização do sistema na rede e domínio do cliente;
- Definição do nível de proteção;
- Instalação do último sistema operativo recomendado pelo fabricante;
- Integração com AD;
- Configuração de alertas de e-mail, SNMP conforme necessário;
- Implementação de partilha de CIFS shares, NFS;
- Implementação de políticas de Quotas;
- Integração com solução NAS proposta;
- Instalação\Configuração de Software de Monitorização;
- Testes de funcionamento;
- Condução de uma transferência de conhecimento.

Declarações dos Fabricantes Exigidas:

Os equipamentos a adquirir neste Concurso irão integrar a Solução actual existente no DataCenter do Município de Abrantes dos construtores DELL e Unisys.

No sentido de evitar qualquer questão com violação de propriedade intelectual e garantir a compatibilidade total com os equipamentos existentes, o Proponente deve de submeter juntamente com a Proposta declaração dos construtores Dell EMC e Unisys para comprovar que estão autorizados a prestar os serviços pretendidos.