LAURA MARIA JESUS RODRIGUES

Assinado de forma digital por LAURA MARIA JESUS RODRIGUES
Dados: 2025.06.02 09:48:41 +01'00'

CONCURSO PÚBLICO

(Nos termos do Código dos Contratos Públicos, na sua atual redação)

CP/S.00001.2025

Caderno de Encargos

Renovação e upgrade de solução de segurança - antivírus, firewall e IOT

smas torres vedras

CADERNO DE ENCARGOS

PARTE I

DISPOSIÇÕES GERAIS

Cláusula 1.ª

Definições

Para efeitos do presente Caderno de Encargos, apresentam-se ou adotam-se as seguintes definições:

a) **Adjudicatário/a** – entidade convidada a quem se adjudica a execução do contrato;
b) **CCP** – Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, com a sua atual redação;
c) **Contrato** – contrato a celebrar entre a entidade adjudicante e o/a adjudicatário/a nos termos do presente Caderno de Encargos;
d) **Entidade Adjudicante** – Serviços Municipalizados de Água e Saneamento de Torres Vedras (SMASTV).

Cláusula 2.ª

Caderno de Encargos

O presente Caderno de Encargos estabelece as condições jurídicas, técnicas e económicas do contrato a celebrar no âmbito do presente procedimento.

Cláusula 3.ª

Objeto

A contratação tem por objeto a **aquisição de renovação e upgrade de solução de segurança - antivírus, firewall e IOT,** com os Códigos **CPV's 72910000-2 - Serviços informáticos de segurança, 72267000-4 Serviços de manutenção e reparação de software e 32420000-3 Equipamento de rede.**

Cláusula 4.ª

Contrato

1. Conforme o que dispõe o artigo 94.º do CCP, o contrato é reduzido a escrito e composto pelo respetivo clausulado contratual e os seus anexos, que integra o seguinte:
   a) Os suprimentos dos eventuais erros e omissões do Caderno de Encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo Órgão competente para a decisão de contratar;
   b) Os esclarecimentos e eventuais retificações relativos ao Caderno de Encargos;
   c) O presente Caderno de Encargos;
   d) A proposta adjudicada;
   e) A referência à caução prestada pelo adjudicatário/a, quando aplicável;
   f) A referência à liberação da caução nos termos do disposto no artigo 295.º, nos casos em que esta é exigida;
   g) Os eventuais esclarecimentos sobre a proposta adjudicada prestados pelo/a adjudicatário/a.

2. Em caso de divergência entre os documentos referidos no número anterior e o clausulado do contrato, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do CCP e aceites pelo/a adjudicatário/a nos termos do disposto no artigo 101.º desse mesmo diploma legal.

3. Em caso de divergência entre o Convite e o Caderno de Encargos, prevalece este último.

Cláusula 5.ª

Prazo de execução do contrato

Sem prejuízo do disposto na Cláusula 18.ª do presente Caderno de Encargos, o contrato tem uma duração de **36 (trinta e seis) meses**, iniciando a sua vigência no dia subsequente à data da última assinatura.

Cláusula 6.ª

Preço base

1. O preço base - sendo o entendido como preço máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações objeto do contrato a celebrar - é **223 982,98 € (duzentos e vinte e três mil, novecentos e oitenta e dois euros e noventa e oito**

cêntimos), acrescido de IVA à taxa legal em vigor, sendo este dividido da seguinte forma, por CPV:

CPV	Valor (S/IVA)
72910000-2 - Serviços informáticos de segurança (Itens 3.4, 3.5, 3.6, 3.7, 3.8, todo o capítulo 4 e 6.1.1 do Anexo I do Programa do Procedimento)	146 540,21 €
72267000-4 - Serviços de manutenção e reparação de software (Item 6.2.1 do Anexo I do Programa do Procedimento)	16 226,64 €
32420000-3 - Equipamento de rede (Itens dos capítulos 1, 2, 3.1, 3.2, 3.3 e 5.1 do Anexo I do Programa do Procedimento)	61 216,13 €

2. O valor apurado no número anterior foi obtido, tendo por base consulta preliminar, realizada nos termos do art.º 35-A do CCP.

3. Nos termos da alínea d) do n.º 2 do artigo 70.º do CCP será excluída a proposta caso apresente preço contratual superior ao preço base.

OBRIGAÇÕES CONTRATUAIS

Cláusula 7.ª

Obrigações principais do/a adjudicatário/o

Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos, ou nas cláusulas do contrato, decorrem para o/a adjudicatário/a as seguintes obrigações principais:

a) Executar o contrato de acordo com as cláusulas técnicas do presente Caderno de Encargos e da proposta adjudicada;
b) Cumprimento dos prazos de disponibilização do licenciamento e do hardware propostos, de acordo com o indicado na proposta, sem prejuízo dos prazos máximos fixados na Cláusula 19.ª do presente Caderno de Encargos.

Cláusula 8.ª

Trabalhadores Afetos à Prestação de Serviços

1. O prestador de serviços obriga-se a cumprir o disposto no artigo 419.º-A do CCP, aplicável por remissão do n.º 2 do artigo 451.º do mesmo diploma, nos termos do qual:

a) Sendo a vigência do contrato superior a 1 ano, os trabalhadores afetos ao contrato prestam a sua atividade em regime de contrato de trabalho sem termo;

b) Sendo a vigência do contrato igual ou inferior a 1 ano, os trabalhadores afetos ao contrato podem prestar a sua atividade em regime de contrato de trabalho a termo, não podendo o vínculo laboral ter duração inferior à vigência do contrato de prestação de serviços.

2. São aplicáveis as exceções previstas nos n.ºs 3 e 4, do artigo 419.º-A do CCP.

Cláusula 9.ª

Vinculação ao Código de Conduta para Entidades Fornecedoras

1. O/A contratante, de acordo com o Código de Conduta para Entidades Fornecedoras, que se encontra em anexo ao presente caderno de encargos, compromete-se a adotar padrões éticos, criar um ambiente de trabalho que assegure a qualidade e promova a segurança e saúde no trabalho, o respeito, a integridade, a igualdade de tratamento, a proteção e preservação do ambiente, a segurança da informação dos SMASTV e das suas Partes Interessadas.
2. Neste âmbito, constituindo o cumprimento do Código de Conduta uma obrigação essencial do contrato, durante e após a sua execução, o/a Cocontratante compromete-se a:
   a) Observar o princípio da legalidade;
   b) Respeitar os direitos fundamentais dos trabalhadores e trabalhadoras;
   c) Assumir os compromissos de gestão ali constantes;
   d) Promover, preservar e proteger o ambiente, assim como assegurar o desenvolvimento sustentável.
3. Qualquer incumprimento do referido Código constitui uma violação grave das obrigações contratuais, com as consequências previstas no Código dos Contratos Públicos.
4. A entidade adjudicante reserva-se o direito de monitorizar o cumprimento das disposições do Código de Conduta por parte do/a cocontratante, podendo, para tal, solicitar informações ou esclarecimentos sempre que tal se revele necessário.

Cláusula 10.ª

Proteção de dados

1. O/a adjudicatário/a, durante a vigência do Contrato e após a sua cessação, obriga-se a:

   a) Observar, escrupulosamente, o regime legal da proteção de dados pessoais, aprovado pelo Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de

2016, e pela Lei n.º 58/2019 de 8 de agosto, empenhando-se em proceder a todo o tratamento de dados pessoais que venha a mostrar-se necessário ao desenvolvimento do Contrato no estrito e rigoroso cumprimento da Lei;

b) Manter a confidencialidade sobre todos os documentos, dados e informações obtidos em virtude da execução do Contrato, que se refiram aos SMASTV e aos/às seus/suas Trabalhadores/as.

2. Ao/À adjudicatário/a cabem as seguintes obrigações:

a) O tratamento dos dados pessoais obedecerá às instruções documentadas do/a responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, exceto se for obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o/a responsável pelo tratamento desse requisito, antes de proceder a essa transferência, salvo se tal informação for proibida por motivos de interesse público;
b) Garante que as pessoas autorizadas a tratar dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
c) Adota todas as medidas de segurança do tratamento, de acordo com o que for mais adequado ao caso:
    i) a pseudonomização e a cifragem de dados pessoais;
    ii) a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
    iii) capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico;
    iv) têm um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento
d) Apenas contratará outro/a subcontratante se o/a Responsável pelo Tratamento o autorizar ou, em caso de autorização prévia, comunicará ao/à Responsável pelo Tratamento a contratação de um/uma subcontratante que deverá respeitar todas as obrigações de tratamento decorrentes do RGPD e da restante legislação relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais;
e) Prestará assistência ao/à responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados, tendo em vista o exercício dos seus direitos;

f) Prestará assistência ao/à responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações de segurança no tratamento, notificação à autoridade de controlo e aos/às titulares em caso de violação de dados pessoais, avaliação de impacto sobre a proteção de dados e consulta prévia, tal como previstas nos artigos 32.º a 36.º do RGPD, com as especificidades da Lei n.º 58/2019 de 8 de agosto, tendo em conta a natureza de tratamento e a informação ao dispor do subcontratante;
g) Dependendo da opção do/a responsável pelo tratamento, apagará ou devolverá todos os dados pessoais depois de concluída a prestação de serviços relacionada com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros;
h) Disponibilizará ao/à responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações que impendem sobre o subcontratante e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo/a responsável pelo tratamento ou por outro/a auditor/a por este mandatado; e
i) Compromete-se a informar imediatamente o/a responsável pelo tratamento se considerar que alguma instrução viola o RGPD ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados.

3. O incumprimento destes deveres e a verificação de inexistência de garantias de *compliance* é fundamento de resolução do presente contrato com justa causa.

OBRIGAÇÕES DA ENTIDADE ADJUDICANTE

Cláusula 11.ª

Preço contratual

1. Pelo cumprimento dos serviços objeto do contrato bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, os SMASTV devem pagar ao/à adjudicatário/a o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor nas condições da cláusula seguinte.

2. O preço a pagar, inclui todos os custos e encargos cuja responsabilidade não esteja expressamente atribuída ao contraente público.

Cláusula 12.ª

Condições de pagamento

1. As quantias devidas pelos SMASTV nos termos da cláusula anterior devem ser pagas no prazo de 30 (trinta) dias a contar da data de entrega das respetivas faturas. As faturas devem ser emitidas em formato eletrónico, conforme o artigo 299.º-B do CCP, indicando o número sequencial do compromisso correspondente, o fornecimento realizado, as quantidades, os preços unitários e o valor total. Deve ser emitida uma fatura distinta para cada número sequencial de compromisso existente, assegurando uma correspondência direta entre os compromissos assumidos e as respetivas faturas. As faturas só podem ser emitidas após o vencimento da obrigação a que se referem.

2. A fatura deverá ser remetida em formato eletrónico e o envio para o endereço de correio eletrónico comunicado pelos SMASTV após teste de validação do ficheiro XML, acompanhado de um PDF com a imagem da fatura que deverá ser certificada digitalmente e ter os dados que obrigatoriamente devem constar da fatura.

3. Nas circunstâncias referidas no número anterior deve, antes do envio da primeira fatura pelo/a adjudicatário/a, ser efetuado obrigatoriamente um teste para despistar possíveis problemas de formato e ajustes de campos extra.

4. Sem prejuízo do disposto nos números anteriores, em caso de discordância por parte dos SMASTV quanto aos elementos e valores indicados na(s) fatura(s), devem estes comunicar ao/à adjudicatário/a os respetivos fundamentos, ficando este 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 transferência bancária ou, na sua impossibilidade, por envio de cheque.

INCUMPRIMENTOS

Cláusula 13.ª

Cessão da Posição Contratual do Fornecedor

1. Além da situação prevista na alínea a) do n.º 1 do artigo 318.º do CCP, o/a adjudicatário/a pode ceder a sua posição contratual, na fase de execução do contrato, mediante autorização da Entidade Adjudicante.

2. Para efeitos da autorização a que se refere o número anterior, o/a adjudicatário/a deve apresentar uma proposta fundamentada e instruída com os documentos previstos no n.º 2 do artigo 318.º do CCP.

3. A Entidade Adjudicante deve pronunciar-se sobre a proposta o/a adjudicatário/a no prazo de 30 (trinta) dias a contar da respetiva apresentação, desde que regularmente instruída, considerando-se o referido pedido rejeitado se, no termo desse prazo, o mesmo não se pronunciar expressamente.

4. Em caso de incumprimento pelo/a adjudicatário/a que reúna os pressupostos para a resolução do contrato, este cederá a sua posição contratual ao concorrente do procedimento pré-contratual que antecedeu a celebração do contrato que venha a ser indicado pela Entidade Adjudicante, de acordo com o estabelecido no artigo 318.º-A do CCP.

5. A cessão da posição contratual a que se refere o número anterior opera por mero efeito do ato da Entidade Adjudicante, sendo eficaz a partir da data por este indicada.

Cláusula 14.ª

Força maior

1. Não podem ser impostas penalidades, 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, circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham; 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; 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; manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais; 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; avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem; 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.

DISPOSIÇÕES FINAIS

Cláusula 15.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 CCP, 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 16.ª

Contagem dos prazos

Os prazos previstos para execução do contrato são contínuos, correndo em sábados, domingos e dias feriados, nos termos do disposto no artigo 471.º do CCP.

PARTE II

CLÁUSULAS TÉCNICAS

Requisitos técnicos, enquanto aspetos mínimos das prestações do contrato não submetidas à concorrência

Cláusula 17.ª

Solução tecnológica

1.1. Solução existente

1.1.1. Visão geral:

Os serviços do SMASTV encontram-se localizados em diversos locais geograficamente separados, mas conectados por tecnologia IP, permitindo as comunicações entre os diversos departamentos funcionais da instituição.

Os locais relevantes ao presente concurso são:

- Localização A;
- Localização B;
- Localização C.

1.1.2. Infraestrutura de comunicações:

Os SMASTV possuem à data uma infraestrutura de rede suportada por equipamentos do fabricante Cisco/Meraki, tirando total partido das funcionalidades inerentes à gestão centralizada da infraestrutura proporcionadas pela plataforma Cloud Meraki.

1.1.2.1. Diagrama de rede atual:

O seguinte diagrama ilustra a solução atual:

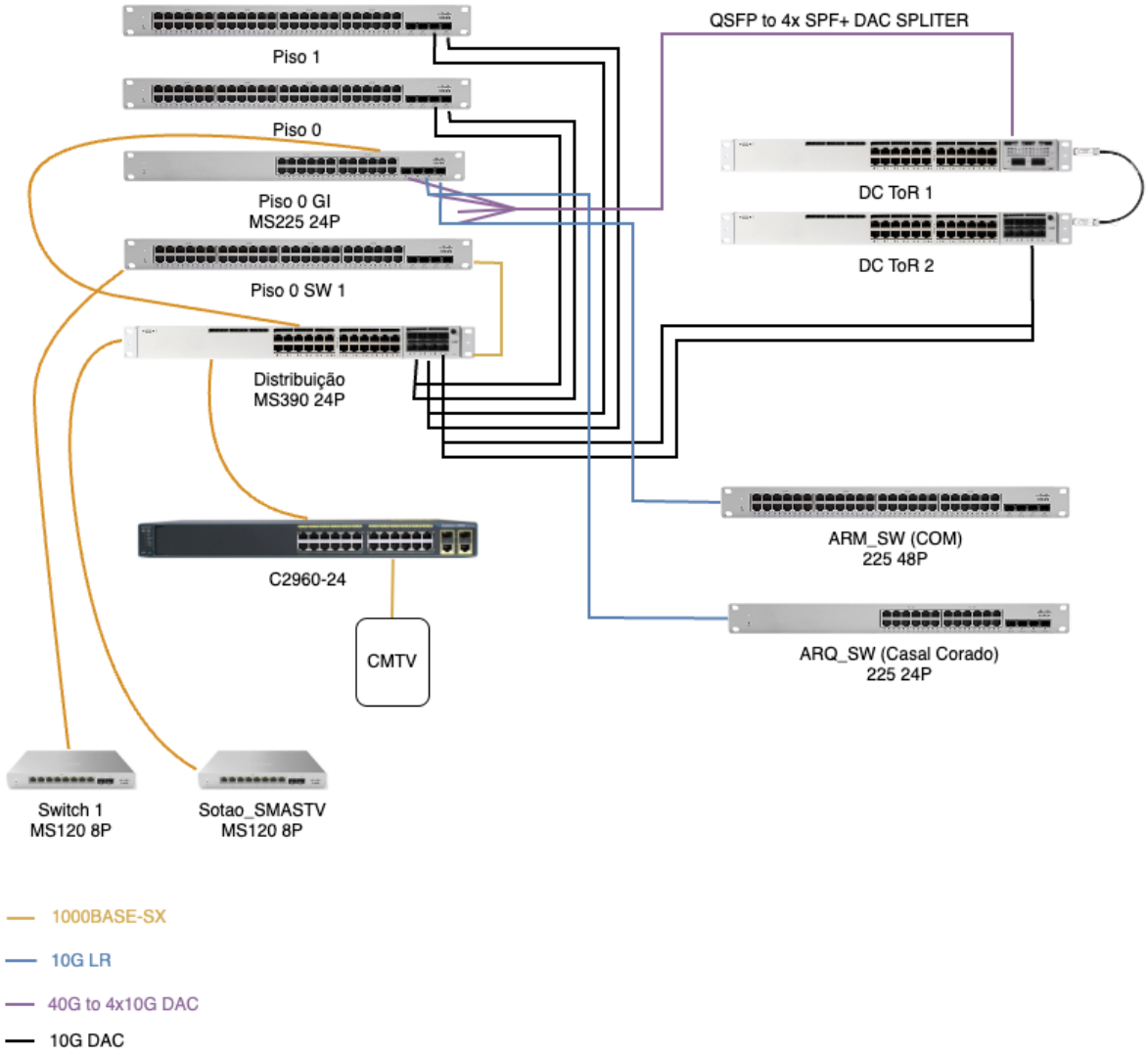

Figura 1 - Solução existente

A infraestrutura de rede local dos SMASTV é baseada maioritariamente em equipamentos do fabricante Cisco/Meraki.

Os equipamentos identificados como Piso 1, Piso 0, Piso 0 GI, Piso 0 SW1, Distribuição e C2960-24 encontram-se localizados num único bastidor de comunicações existente no atual centro de dados do SMASTV, na Localização A.

Os equipamentos identificados como DC ToR 1 e DC ToR 2, encontram-se também no atual centro de dados do SMASTV, na Localização A, mas em operação num segundo bastidor dedicado aos sistemas de computação.

1.1.3. Infraestrutura de Cibersegurança:

Os SMASTV possuem requisitos de segurança de informação que não podem ser relegados para segundo plano. A confidencialidade da informação deverá ser uma garantia e obrigação de qualquer serviço municipal. A cibersegurança será um pilar fundamental para estratégia, arquitetura e modelo de serviço que se pretende para os SMASTV, de acordo com os pilares da segurança de informação, sendo estes a confidencialidade, integridade e disponibilidade.
Para respondermos a esses requisitos, assim como, para garantir as exigências da atualidade no que toca à ciber-resiliência e maturidade em cibersegurança dos SMASTV, o proponente deverá apresentar uma solução de um fabricante como parceiro tecnológico, líder de mercado neste tipo de soluções.

Os SMASTV possuem atualmente um cluster de firewalls do fabricante Palo Alto Networks, assente na plataforma PA-450, com suporte e subscrições válidas até 7 de julho de 2025.

Adicionalmente, para proteção dos seus endpoints, os SMASTV possuem uma solução da Palo Alto Networks, o Cortex XDR Pro, licenciada para 200 endpoints até 30 de junho de 2025.

Uma vez que as firewalls referidas anteriormente já se encontram aquém das necessidades da organização, pretende-se a renovação desta solução para equipamentos com maior performance, de acordo com as especificações apresentadas de seguida. Relativamente à proteção de endpoint, o que se pretende é a renovação da solução existente por 3 anos e acrescentar-lhe algumas funcionalidades de forma a providenciar uma maior proteção, conforme também explicitado mais à frente neste documento.

Para garantir que a solução de segurança é transversal, adotando o contexto de plataformização, com vista ao aumento do nível de segurança global e de uma simplificação das operações, pretende-se que todas as soluções de segurança sejam do mesmo fabricante.

Por forma a garantir a qualidade das soluções apresentadas é obrigatório, sob pena de exclusão, a entrega com a proposta de uma Declaração do fabricante das soluções de segurança fazendo prova que o mesmo tem conhecimento da proposta apresentada pelo concorrente, certificando que o concorrente possui as competências necessárias para implementação e suporte da solução.

1.2. Solução Pretendida - Infraestrutura de Rede

1.2.1. Considerações gerais:

Este concurso enquadra-se numa renovação de uma determinada área dos SMASTV. Não se contemplando, como critério, a substituição de todo o parque de equipamentos ativos de rede instalados e atualmente em funcionamento, excluindo do âmbito da mesma, um conjunto de equipamentos que foram adquiridos ao longo dos últimos anos e que ainda se consideram úteis, protegendo-se assim, o investimento já realizado.

Considerando que a implementação de uma rede de comunicações com heterogeneidade de fabricantes apresenta um risco real no aumento da perturbação dos serviços que suporta, será fundamental assegurar que os equipamentos propostos para cada uma das componentes (infraestrutura de rede e segurança) sejam de um único fabricante, que estes garantam conformidade com os mais recentes standards do mercado e que possuam capacidade de evolução e flexibilidade para acompanhar as crescentes necessidades dos SMASTV, potenciando desta forma a longevidade da solução e maximização do investimento a realizar.

A solução deve ser implementada por uma equipa especializada acompanhada tanto de integradores como pelo fabricante, com experiência e conhecimento das necessidades dos SMASTV, constituindo uma garantia de uma integração sem disrupção de serviço e de uma implementação de uma infraestrutura estável.

A equipa do integrador deve possuir certificação e credenciação do fabricante, bem como, experiência em intervenções análogas e em instalações de semelhante complexidade.
Todo o processo de integração deverá ser previamente planeado e aprovado, para que em caso imperativo de downtime, o mesmo seja o mais curto possível. O horário para a realização dos trabalhos será a definir posteriormente pelos SMASTV.

Esta renovação deverá assegurar a implementação de uma solução tecnologicamente atual, com produtos e equipamentos que representem o atual estado da arte, permitindo uma clara melhoria na qualidade e fiabilidade das infraestruturas de comunicações existentes, bem como a sua evolução e continuidade para os próximos anos.
Deverá ser dado especial enfase à segurança da informação, orientando as soluções propostas a este fim.

O concorrente deverá apresentar obrigatoriamente com a proposta, mencionando a referência do presente concurso, uma declaração do fabricante em como é revendedor autorizado e possui todas as certificações para a prestação de serviços de implementação e assistência técnica nas áreas/equipamentos/software constantes na sua proposta. E garantir na totalidade a integração com as plataformas Meraki e PaloAlto existentes.

O adjudicatário compromete-se a adquirir os equipamentos via canais autorizados, que estes serão novos e estarão nas suas embalagens originais.

Todos os produtos deverão estar sujeitos a uma garantia do fabricante e todo o software será original e licenciado de acordo com a infraestrutura proposta para os SMASTV.

1.2.2. Descrição:

Pretende-se dotar a infraestrutura de rede local existente de uma maior capacidade de redundância, resiliência e velocidade de transferência de dados.

Os objetivos gerais do projeto são:

a) CORE/DATACENTER
   i. Consolidação e centralização das conetividades dos bastidores de acesso existentes;
   ii. Elevar a disponibilidade, largura de banda e redundância de toda a solução de comunicação de dados;
   iii. Interligação, com recurso a ligação 40Gbps sobre fibra ótica monomodo, a um dos novos equipamentos do Datacenter DC-DR.

b) Datacenter DC-DR
   i. Fornecimento, instalação e configuração de dois novos equipamentos, configurados em modo de cluster (dois equipamentos independentes, mas que em conjunto permitam efetuar agregação multi-chassis de interfaces);
   ii. Os novos equipamentos deverão ser interligados com recurso a duas ligações 100Gbps;
   iii. Interligação, com recurso a duas ligações 40Gbps sobre fibra ótica monomodo, aos novos equipamentos do CORE/DATACENTER;
   iv. Reconfiguração de um dos dois switches ToR atualmente existentes (Cisco C9300-24UX) para instalação na função de ToR 1/10Gb RJ45.

c) Acesso

i. Redesenho de conetividades, criando um stack com os equipamentos já existentes no bastidor de comunicações do centro de dados da Localização A;

ii. Movimentação e otimização de switches de acesso, procurando a criação de redundância e a diminuição de saltos necessários para atingir os equipamentos de CORE/DISTRIBUIÇÃO;

iii. Interligação 10Gb sobre fibra ótica monomodo entre os sites Localização B e Localização C, aumentando a redundância da solução.

Pretendendo os SMASTV um solução chave-na-mão, a proposta deverá incluir todos os equipamentos, acessórios e serviços necessários para atingir os objetivos de projeto.

O concorrente poderá reutilizar equipamentos já existentes (switches, cabos DAC, transceivers) desde que a compatibilidade com os equipamentos propostos seja assegurada.

1.2.3. Diagrama da solução pretendida:

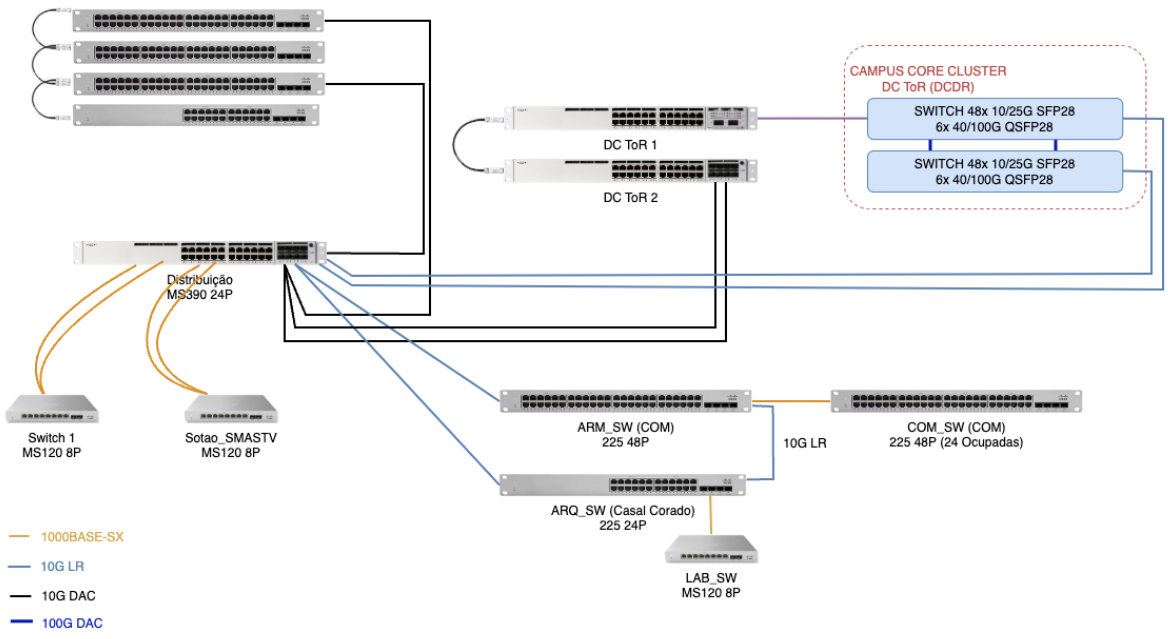

Figura 2 - Solução pretendida

Os equipamentos pretendidos encontram-se representados na figura com a legenda "SWITCH 48x 10/25G SFP28 6x 40/100G QSFP28".

1.2.4. Especificação técnica:

1.2.4.1. SWITCH TIPO 1:

Os switches deverão ter capacidade para suportar as seguintes características e funcionalidades mínimas obrigatórias:

Hardware

a) Tamanho máximo 1 Rack Units (RU);
b) Pelo menos 48 portas 1/10/25G Ethernet com interfaces SFP+;
c) Pelo menos 6 portas 40/100G Ethernet com interfaces QSFP28;
d) Portas na traseira do equipamento:
    i. 1 porta para gestão out-of-band RJ-45;
    ii. 1 porta USB;
    iii. 1 porta série RS-232.
e) Switch L2 e L3 "line-rate", sem contenção em todas as portas;
f) Capacidade de comutação de pelo menos 3,6Tbps e 1,2Bpps (mil milhões de pacotes por segundo);
g) Opção de "Airflow" frente-para-trás e trás-para-frente:
    i. Equipado para operar no modelo de fluxo de ar frente-para-trás.
h) Fontes de alimentação com eficiência "80 Plus Platinum";
i) Fontes de alimentação redundantes e "hot-swappable":
    i. Equipado com fonte de alimentação redundante com 650W.
j) Módulos de refrigeração redundantes e "hot-swappable";
k) Consumo típico não deve exceder 375W;
l) Consumo máximo não deve exceder 600W;
m) Suporte para 1,792,000 rotas IPv4;
n) Suporte para 512,000 entradas MAC;
o) Suporte para 128,000 rotas Multicast;
p) CPU com pelo menos 4 cores;
q) Memória de sistema com pelo menos 16GB;
r) Drive SSD com pelo menos 128GB;
s) Deve dispor de um buffer partilhado não inferior a 40MB partilhado;
t) Todas as portas devem suportar IEEE 802.1ae MAC Security (MACsec);

u) Deve suportar a ligação de módulos remotos (extensões ao fabric ou satélites) para aumentar a escalabilidade em quantidade e tipo de portos. A gestão dos módulos remotos e respetivas portas deve ser feita no switch base e não nos módulos remotos, pelo que, independentemente da quantidade de módulos remotos, a solução deve apresentar sempre apenas um "management plane";
v) MTBF superior a 300 000 horas.

Sistema Operativo

Os switches devem suportar as seguintes funcionalidades, ou equivalente:

a) O sistema deve suportar upgrades de software em serviço (In-service upgrade);
b) Funcionalidades L2 (ou equivalentes):
   i. 4096 VLANs;
   ii. Port-Channel com membros em equipamentos distintos (Multi-Chassis EtherChannel);
   iii. Spanning Tree Protocol:
      - IEEE 802.1w;
      - IEEE 802.1s Multiple Spanning Tree (MST);
      - Edge port and edge-port trunk;
      - Extensions: Bridge Protocol Data Unit (BPDU) guard, BPDU filtering, bridge assurance, loop guard, e root guard.
   iv. MAC addresses unicast e multicast estáticos;
   v. IEEE 802.3x Flow Control;
   vi. IEEE 802.1AB Link Layer Discovery Protocol (LLDP);
   vii. Maximum transmission unit (MTU) configuráveis e suporte de jumbo frames;
   viii. Automatic medium-dependent-interface crossover (auto-MDIX);
   ix. Unidirectional Link Detection (UDLD).
c) Funcionalidades L3 (ou equivalentes):
   i. IPv4:
      - Rotas estáticas;
      - BGP, OSPFv2, e Intermediate System to Intermediate System (ISIS);
      - VRF-Lite e VRF route leaking;
      - VRRP;
      - Bidirectional Forwarding Detection (BFD);

- Dynamic Host Configuration Protocol (DHCP) relay.

ii. IPv6:
- Rotas estáticas;
- BGP e OSPFv3;
- VRF-Lite e VRF route leaking;
- DHCP relay.

iii. 64-way ECMP;

iv. User-configurable MAC addresses (16) em interfaces routed.

d) Funcionalidades Multicast (ou equivalentes):
i. Interior Gateway Management Protocol (IGMP) v1, v2 e v3;
ii. IGMP snooping;
iii. Protocol-Independent Multicast (PIM) sparse mode (PIM-SM) e Any Source Multicast (ASM);
iv. Anycast Routing Protocol (Anycast RP);
v. Multicast Source Discovery Protocol (MSDP).

e) Funcionalidades para alta-disponibilidade (ou equivalentes):
i. Isolamento de falhas por processo;
ii. ISSU;
iii. Process patching;
iv. Stateless process restart;
v. Stateful supervisor switchover;
vi. Online insertion and removal (OIR) de módulos sem disrupção de tráfego.

f) Funcionalidades de virtualização:
i. VXLAN gateway;
ii. VXLAN bridging;
iii. VXLAN routing.

g) Funcionalidades de segurança (ou equivalentes):

i. ACLs Ingress e egress utilizando campos Layer 2, 3, e 4:
- Extended ACLs, MAC addresses, port ACLs (PACLs), VLAN ACLs (VACLs), e routed ACLs (RACLs).

ii. ACL counters;

iii. Storm control:

- Broadcast, multicast, e unknown unicast.

iv. User-configurable Control-Plane Policing (CoPP);
v. Authentication, authorization, e accounting (AAA):

- Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Microsoft MS-CHAP, e MS-CHAPv2;
- Capacidade para desabilitar role-based access control (RBAC) e usar autenticação de servidor AAA;
- Integração de Role-based access control (RBAC) para substituir "privilege levels";
- Logging;
- VRF context support;
- Suporte de Lightweight Directory Access Protocol (LDAP).

vi. RADIUS;
vii. RBAC;
viii. TACACS+.

h) Tipo de Interfaces:

i. Layer 2 switch port:

- Access e trunk (VLAN list and native VLAN tagged and untagged).

ii. Layer 3 routed;
iii. Loopback interface;
iv. Switched virtual interface (SVI);
v. PortChannel:

- Static mode;
- IEEE 802.3ad LACP;
- Load balancing;
- Member link ping;
- Minimum number of links.

i) Funcionalidades de QoS:

i. Até 4 queues por porta;
ii. Classificação ACL-based;
iii. Queuing:

- Strict priority;
- Weighted Round-Robin (WRR).

vi. Marking and classification:

- Differentiated services code point (DSCP) on switch;
- Class of service (CoS);
- CoS preservation for Remote Direct Memory Access;
- (RDMA) over Converged Enhanced Ethernet (RoCEE).

vii. Policing:

- Ingress.

viii. Explicit congestion notification (ECN);

ix. Weighted Random Early Detection (WRED);

x. Suporte de Priority flow control (PFC) até 3 classes PFC.

j) Funcionalidades de Gestão (ou equivalentes):

i. POAP (power on auto provisioning);

ii. Configuration rollback;

iii. Configuration session manager;

iv. Cliente FTP, SFTP e TFTP;

v. Network Time Protocol (NTP):

- Client, peer, server, ACL e autenticação.

vi. Cliente de Remote copy (RCP) e secure copy (SCP);

vii. Remote monitor (RMON);

viii. Envio de mensagens de alerta referentes a falhas de hardware para o NOC do fabricante;

ix. Simple Network Management Protocol (SNMP) v1, v2 e v3;

x. Syslog;

xi. Virtual terminal (vty);

xii. Secure Shell (SSH) v2 (client e server);

xiii. Telnet (client e server);

xiv. Acesso à Shell (Linux) do sistema operativo, com possibilidade de scripting.

k) Extensibilidade e programabilidade:

i. Linux tools - Bash shell access;

ii. Python shell;
iii. Extensible Messaging and Presence Protocol (XMPP) cliente;
iv. API com suporte para Remote Procedure Calls (RPCs; JSON; XML) sobre HTTP e HTTPS;
v. Plug-in para OpenStack;
vi. XML (Netconf).

l) Standards:

i. IEEE 802.1D Bridging and Spanning Tree;
ii. IEEE 802.1p QoS/CoS;
iii. IEEE 802.1Q VLAN Tagging;
iv. IEEE 802.1w Rapid Spanning Tree;
v. IEEE 802.1s Multiple Spanning Tree Protocol;
vi. IEEE 802.1AB Link Layer Discovery Protocol;
vii. IEEE 802.3ad Link Aggregation with LACP;
viii. IEEE 802.3x Flow Control;
ix. IEEE 802.3ab 1000BASE-T;
x. IEEE 802.3z Gigabit Ethernet;
xi. IEEE 802.3ae 10 Gigabit Ethernet;
xii. IEEE 802.3ba 40 Gigabit Ethernet;
xiii. RFC 2460 IPv6;
xiv. RFC 2461 Neighbor Discovery for IPv6;
xv. RFC 2462 IPv6 Stateless Address Autoconfiguration;
xvi. RFC 2463 ICMPv6.

Equipamento de referência: N9K-C93180YC-FX3

1.3. Solução Pretendida – Segurança

1.3.1. Considerações gerais:

Pretende-se a substituição dos atuais equipamentos de firewall de perímetro, com a aquisição de um novo cluster de firewall composto por 2 equipamentos com as características de Next Generation Firewall e que deverão cumprir as especificações presentes nos pontos seguintes.

Com o cluster de firewalls deverão ser fornecidos 2 SFP+ de 10GB LR (1 para cada nó do cluster), para operação sobre fibra ótica monomodo, que deverão ser do mesmo fabricante das appliances para garantir compatibilidade e garantia de suporte.

Deverá ser disponibilizado 1TB de espaço em cloud para funcionar como datalake da solução para logs ou outras funcionalidades da solução (conforme solicitado abaixo nas especificações de IoT da solução).

O Fabricante das soluções de firewall de perímetro, deverá ser líder no quadrante de Enterprise Network Firewalls da Gartner pelo menos nos últimos 5 anos.

A solução deverá considerar 3 anos de validade para o suporte e subscrições de software.

1.3.2. Descrição:

Pretende-se dotar a infraestrutura de rede local existente de uma maior capacidade de redundância, resiliência e velocidade de transferência de dados.

Os objetivos gerais do projeto são:

a) Substituição do Atual Cluster de Firewalls Perimetrais:

   i. Fornecimento, instalação e configuração de dois novos equipamentos, configurados em modo redundante, um em cada datacenter;
   ii. Interligação dos equipamentos de firewall com uma ligação 10Gbps sobre fibra ótica monomodo;
   iii. Validação e consolidação das atuais configurações, estabelecendo as boas práticas aplicáveis à instituição;
   iv. Os novos equipamentos de Firewall deverão ligar à infraestrutura de comunicações existente com recurso a ligações 10Gbps, duas por equipamento de Firewall. No Datacenter DR, cada uma das ligações deverá terminar num membro distinto do novo Cluster de CORE/DATACENTER, garantindo a correta redundância e resiliência a falha.

b) Renovação das subscrições de segurança de Endpoint Existentes:

   i. Renovação das subscrições Cortex XDR PRO para 200 dispositivos terminais;

   ii. Renovação das subscrições Extended Threat Hunting para 200 dispositivos terminais;

iii. Aquisição e implementação de subscrição Host Insights para 200 dispositivos terminais.

Pretendendo os SMASTV um solução chave-na-mão, a proposta deverá incluir todos os equipamentos, acessórios e serviços necessários para atingir os objetivos de projeto.

O concorrente deverá integrar com os equipamentos já existentes (switches, cabos DAC, transceivers).

1.3.3. Diagrama solução pretendida:

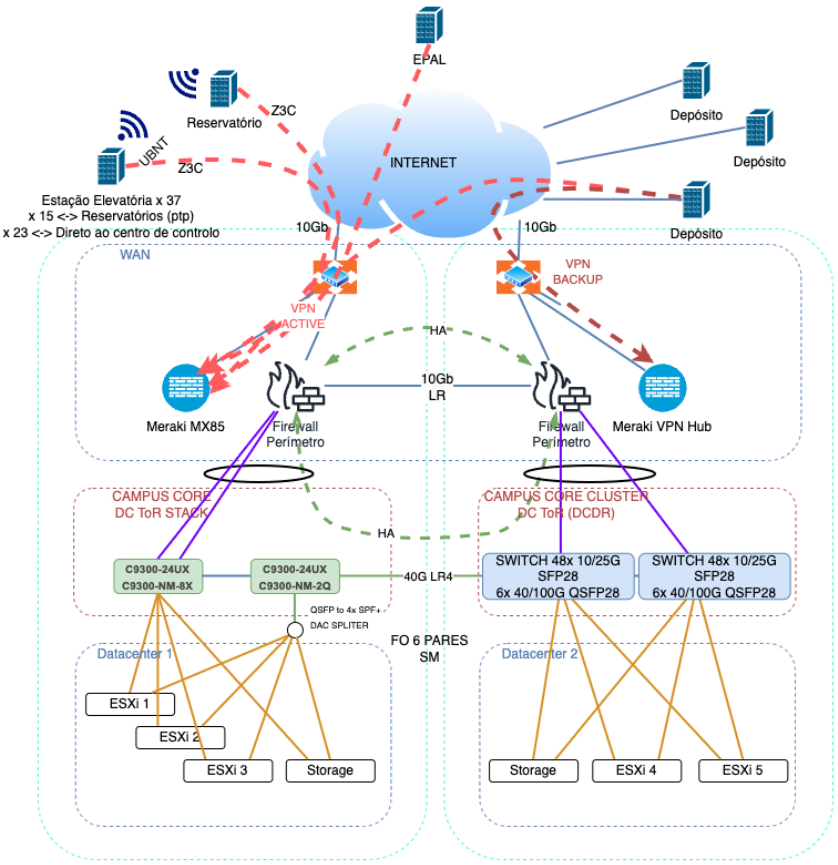

Figura 3 - Solução pretendida

1.3.4. Especificação técnica:

1.3.4.1. FIREWALL DE PERÍMETRO:

Os equipamentos de Firewall de Perímetro deverão possuir as seguintes características e funcionalidades mínimas obrigatórias:

Hardware (obrigatório dentro do mesmo equipamento):

a) Número de portas 10Gbit/s SFP+ >= 4;
b) Número de portas Gigabit SFP 1Gbit/s >= 6;
c) Número de portas Gigabit 1/2,5/5 Gbit/s POE >= 4;
d) Número de portas 1Gbit/s RJ45 >= 8;
e) Porta de consola RJ45;
f) Porta Micro USB serial consola >= 1;
g) Disco rígido SSD >= 120GB;
h) A appliance de FW deverá ter uma arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção;
i) Deverá estar garantido que a appliance de FW quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa;
j) Fonte de alimentação redundante incluída.

Performance:

a) Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção) >= 8,5 Gbps;
b) Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) >= 4,5 Gbps;
c) Performance da appliance com a funcionalidade de VPN IPSec >= 4,1 Gbps;
d) Número de novas sessões por segundo >= 100 000;
e) Número máximo de sessões >= 945 000.

Gestão:

a) Gestão e administração da própria appliance através de interface web, linha de comandos e API XML;

b) Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio;
c) Na gestão centralizada deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy;
d) Possibilidade de editar configurações pendentes que ainda não foram aplicadas;
e) Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas;
f) Possibilidade de descartar alterações à configuração realizadas;
g) Possibilidade de armazenar diferentes versões da configuração;
h) Na gestão centralizada deve existir a capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada;
i) Na gestão centralizada deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos;
j) Na gestão centralizada deve existir um ponto centralizado para efetuar upgrades e atualizações de versões e assinaturas;
k) Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão;
l) Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas;
m) Deve existir a capacidade de correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds públicas incluindo Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud;
n) Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento;
o) Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça;
p) Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade.

Networking:

a) As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3;
b) Suporte de IEEE 802.1Q;

c) Suporte de iEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo;
d) Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP;
e) Suporte de routing estático;
f) Suporte de DHCP, NAT e PAT;
g) Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas;
h) Capacidade de realizar policy based routing através do IP ou rede de origem;
i) Capacidade de realizar policy based routing através do utilizador ou grupo;
j) Capacidade de realizar policy based routing através do tipo de aplicação;
k) Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo;
l) Permitir a criação de clusters de alta disponibilidade até 6 membros;
m) Suporte para TLS 1.3 e capacidade de desencriptar este tráfego.

Identificação de Utilizadores:

a) Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP;
b) Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory;
c) Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores;
d) Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores;
e) Possibilidade de gerir utilizadores através de API XML;
f) Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local;
g) Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing.

Funcionalidades Gerais de Segurança:

a) Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança;

b) Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança;
c) Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino;
d) Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas;
e) Capacidade de identificação de subfunções dentro de uma aplicação;
f) Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7;
g) Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações;
h) Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP;
i) Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP;
j) Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL;
k) Capacidade de decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling);
l) Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego;
m) Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança;
n) Capacidade de forçar o uso de MFA para acesso a determinados recursos. Deve ser possível configurar políticas que forcem qualquer utilizador em determinada subnet, a utilizar MFA se tentar aceder a um recurso em determinado segmento de rede da organização;
o) Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes.

IDS/IPS:

a) Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças;
b) Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas;

c) Possibilidade de escolher proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos;
d) As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma a que a aplicação de perfis de proteção se possam realizar com base nestas categorias;
e) Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades;
f) Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis;
g) Deve ser possível converter assinaturas snort e suricata para dentro da plataforma;
h) Capacidade de bloquear comunicações C&C desconhecidas, através de análise inline e machine learning, e em tempo real;
i) Capacidade de gerar assinaturas baseadas em payloads do tráfego malicioso que permitam detetar tráfego C&C mesmo que o host C&C seja desconhecido ou mude constantemente.

Antivirus & Anti-Malware:

a) Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C;
b) Capacidade de habilitar mecanismos de DNS sinkholing que permitam intercetar pedidos de resolução de nomes para domínios comprometidos com malware;
c) Capacidade de definir políticas de antivírus, de forma a que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso;
d) Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs);
e) Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possam tomar uma ação no caso de um ficheiro malicioso;
f) Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações;
g) Capacidade de identificar ficheiros não através das suas extensões mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros;

h) Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente;
i) Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro;
j) Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança;
k) Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados;
l) Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing;
m) Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças;
n) Capacidade de detetar e bloquear ameaças em todos e quaisquer portos em vez se basear em assinaturas que se limitam a um conjunto pré-definido de portos.

URL Filtering:

a) Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar (permitir, bloquear, permitir mas advertir, etc);
b) Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud;
c) Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação);
d) Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web;
e) A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet;

f) A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas;
g) Para além de fornecer proteção contra phishing, a solução deve ser capaz de identificar qualquer utilizador, que tente utilizar as suas credenciais corporativas num site externo à organização. Para além de identificar esta situação a solução tem que ser capaz de a prevenir.

DNS Security:

a) A solução deve disponibilizar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos;
b) Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes;
c) A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling);
d) A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS;
e) Este serviço deve permitir identificar quais as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente;
f) A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente;
g) Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas;
h) Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos;
i) Devem ser disponibilizadas as seguintes categorias para construção de políticas: Command and Control Domains, Malware Domains, Dynamic DNS Hosted Domains, Newly Registered Domains, Phishing Domains, Grayware Domains and Parked Domains;
j) A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças;
k) A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas.

Sandboxing:

a) Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma a que se permita o envio desta informação para análise atendendo aos critérios: tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload);
b) Perante uma análise por parte do serviço de Sandboxing na cloud que categoriza a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente);
c) O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios;
d) A tecnologia de Sandboxing tem de ser capaz de inspeccionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP;
e) A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução;
f) Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux;
g) O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida;
h) Em termos de suporte de sistemas operativos Windows emulados deve suportar: Windows XP, Windows 7 e Windows 10;
i) Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS);
j) Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF);
k) Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado;

l) Capacidade de desencriptar malware (unpacker) para utilização na análise estática e machine learning;
m) Disponibilizar capacidade de Intelligent Run-time Memory Analysis, um mecanismo de análise avançada que complementa os mecanismos de análise estáticos e dinâmicos existentes, para detetar e evitar ameaças evasivas de malware;
n) Deve suportar a análise de ficheiros do tipo Open Office XML (OOXML), em tempo-real aplicando analitica de machine learning.

SD-WAN:

a) A plataforma deve incluir um módulo de SD-WAN;
b) A plataforma deve permitir adicionar um overlay de SD-WAN que permita escolher de forma inteligente e dinâmica os links mais apropriados para envio de tráfego;
c) Deve ser possível criar regras de SD-WAN por aplicação e definir os requisitos mínimos para cada link. No caso de os requisitos mínimos não serem cumpridos pelo link em uso, deve ser feito o failover do tráfego automaticamente;
d) Para os links deve ser possível monitorizar e definir regras com base em: latência, jitter e perda de pacotes;
e) A plataforma deve permitir fazer load-sharing através de múltiplos links de forma a melhorar o aproveitamento da largura de banda disponível;
f) As firewalls devem suportar a funcionalidade de zero-touch provisioning;
g) A plataforma deve disponibilizar informação sobre a performance das aplicações e links;
h) Esta funcionalidade deve ser gerida centralmente através de uma única consola;
i) Deve ser suportada a funcionalidade de Packet duplication, o que permite a um equipamento enviar o mesmo pacote em links diferentes. O equipamento que recebe ambos os pacotes deverá descartar o último a chegar;
j) Deve ser suportada a funcionalidade de Forward Error Correction.

Relatórios & Logs:

a) A appliance deve ter a capacidade gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais;
b) Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas;

c) Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf;
d) Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets;
e) Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende;
f) Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento;
g) Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a largo prazo;
h) Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: aplicações mais utilizadas, aplicações de alto risco, informação geral do sistema, estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, recursos do sistema;
i) Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviado ao serviço de sandboxing e equipamentos internos comprometidos;
j) Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma que a partir dos logs criados se possa obter informações de alto nível.

IOT Security:

a) A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT;
b) A firewall deve colecionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede;
c) A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses;

d) O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camara de vigilancia), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo;
e) Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também;
f) Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal;
g) A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas;
h) Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos, etc;
i) O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associadas ao uso/configuração incorreta dos mesmos. Exemplo: uso de credenciais default;
j) Deve existir a possibilidade de o Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB (Cloud Access Security Broker);
k) O repositório de dados deve ter capacidade de armazenamento de logs de 1 TB.

Outras Funcionalidades:

a) Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade;

b) Possibilidade de decifrar tráfego SSL e SSH de forma que se possa estabelecer políticas de desencriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados;
c) Capacidade de criar exceções à desencriptação para determinado tipo de tráfego;
d) Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC);
e) Possibilidade de enviar tráfego após desencriptação para uma interface de port mirror para análise de terceiras partes;
f) Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego;
g) Capacidade de capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção.

Funcionalidades adicionais licenciáveis:

Os equipamentos deverão ter a capacidade de, no futuro, suportar as seguintes funcionalidades de segurança através de licenciamento adicional:

a) Data Loss Prevention:
   i. A plataforma deve disponibilizar um módulo completo de Data Loss Prevention;
   ii. Esta funcionalidade deve ser disponibilizada como um serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente como por exemplo: Financeiros, Legais, Saúde, informação pessoal, etc. A solução deverá também permitir controlar este tipo de documentos de forma evitar a sua exposição ou extravio;
   iii. Este serviço deverá permitir proteger estes documentos das seguintes formas:
      - Prevenir o upload de ficheiros com informação confidencial e/ou sensível para aplicações web não permitidas pela organização;
      - Monitorizar o upload de documentos para aplicações externas permitidas pela organização.
   iv. O serviço deve disponibilizar out-of-the-box pelo menos 380 "data patterns" e deve também disponibilizar perfis que agrupam determinados padrões de forma a simplificar a criação de políticas. Por exemplo, deverá existir um perfil associado com o GDPR de

forma a facilitar a monitorização de documentos que possam contêm informação pessoal de utilizadores;

v. Deverão existir os seguintes perfis out-of-the-box: Bulk CCN, CCPA, Corporate Financial docs, Financial information, GDPR, GLBA, Healthcare, Intellectual Property, Legal, Malware, Personally-Identifiable Information, Profanity, Self Harm e Sensitive content;

vi. A solução deverá ser constantemente atualizada com novos padrões e perfis;

vii. De forma a melhorar o rácio de deteção e eliminar falsos positivos a solução deverá permitir especificar: proximity keywords, níveis de confiança e expressões regulares básicas ou "weighted";

viii. Este serviço deve poder ser consumido por diferentes plataformas do fabricante, nomeadamente, firewalls, serviço SASE (Secure Access Service Edge), CASB (Cloud Access Security Broker) e CSPM (Cloud Security Posture Management). Isto permitirá aplicar políticas de DLP transversais à organização.

1.3.4.2. Solução de Proteção de Endpoint:

Os SMASTV possuem uma solução da Palo Alto Networks, o Cortex XDR Pro, licenciada para 200 endpoints até 30 de junho de 2025.

Pretende-se a renovação da solução existente por 3 anos a contar dessa data e adicionar-lhe um conjunto de funcionalidades que a permitam adequar-se à exigência da sofisticação das ciber-ameaças atuais, de forma a disponibilizar as seguintes funcionalidades:

a) A instalação de, pelo menos, 200 postos de trabalho/servidores (endpoints);
b) Capacidade para ingestão de 33 Gb/dia de logs;
c) Prevenção contra exploits, incluindo aqueles que utilizam vulnerabilidades do tipo Zero-Day;
d) Prevenção contra a execução de malware, sem requerer qualquer conhecimento prévio;
e) Capacidade de restringir a execução de determinados processos;
f) Proteger contra ransomware;
g) Controlar dispositivos USB;
h) Disk Encryption;
i) Host Firewall;
j) Malware Scanning;

k) Módulo de Endpoint Detection and Response (EDR);
l) Módulo de User Entity Behavior Analytics (UEBA);
m) Módulo de Network Traffic Analysis (NTA).

A solução de proteção de endpoint deverá ser do mesmo fabricante da solução de firewall no sentido de manter uma uniformização da plataforma, simplificando as operações e rentabilizando o conhecimento já existente na organização.

A solução proposta deverá cumprir ainda com as especificações presentes nos pontos seguintes.

Gestão:

A solução proposta deverá:

a) Ser gerida através de uma interface gráfica web;
b) Ter uma gestão centralizada baseada em cloud;
c) Permitir que seja utilizado um serviço de logging na cloud para alojar tanto os logs de firewalls como de endpoints para depois poder integrar com vários outros fabricantes através de uma Framework e APIs;
d) Manter um audit log das seguintes ações dos administradores: Isolar máquina, terminar processo, upgrade de agente, uninstall do agente, adicionar/remover artefacto de whitelist e blacklist;
e) Suportar a atualização de software dos agentes de endpoint diretamente a partir da cloud;
f) Poder exportar os seus logs em formato syslog para qualquer solução de gestão de logs.

Prevenção de Exploits:

a) A solução proposta deve suportar proteger processos do sistema operativo e aplicações, com a capacidade de adicionar à lista de aplicações protegidas, aplicações proprietárias, de terceiras partes ou customizadas;
b) A solução proposta deve ser capaz de fornecer prevenção em tempo real contra exploits de qualquer vulnerabilidade aplicacional (incluindo do tipo zero-day ou desconhecidos) através do bloqueio de técnicas de exploits como "Software Logic Flaws", "Memory Corruptions", "DLL Hijacking", "heap spray", "JIT", "ROP", "SEH", etc;
c) A solução proposta deve ser capaz de efetuar prevenção de exploits através do bloqueio de técnicas de exploits sem requerer conectividade com o servidor de gestão e/ou serviço da cloud e sem utilizar assinaturas;

d) Assim que a solução proposta previne ou bloqueia uma técnica de exploit deve parar imediatamente o processo relacionado, coletar informação forense (nome do processo, ficheiro de origem e o caminho, data e hora, dump da memória, versão do sistema operativo, identificação do utilizador, identificação e versão da aplicação vulnerável, etc.) e terminar apenas este processo;
e) A solução proposta deve utilizar módulos de técnicas de exploit para prevenir ou bloquear exploits. Não deve basear a prevenção ou bloqueio de exploits em assinaturas, reputação e heurísticas dos ficheiros;
f) A solução proposta não deve utilizar de forma intensiva os recursos do endpoint ou utilizar técnicas de análise baseada em hardware específico como sandbox local baseado em virtualização de software ou containers. A solução proposta deve ter impacto mínimo no desempenho através da utilização de um agente leve e não intrusivo que pode ser totalmente invisível para o utilizador;
g) A solução proposta deve proteger de forma simultânea todas as aplicações e processos do endpoint contra técnicas de exploit;
h) A solução proposta deve permitir a configuração granular de políticas de prevenção e bloqueio de exploits por utilizador, grupos ou máquina (endpoint) e ter políticas pré-configuradas para os processos mais comuns do sistema Microsoft Windows;
i) A solução proposta deve também conseguir proteger contra exploits para MacOS e Linux como por exemplo "local privilege escalation";
j) Deve ser possível criar exceções de forma manual para técnicas de exploit específicas em processos específicos. Esta funcionalidade deve estar disponível em Windows, Linux e Mac.

Prevenção de Malware:

a) A solução proposta deve suportar proteção contra a execução de executáveis maliciosos;
b) A solução proposta deve garantir a funcionalidade de monitorização ou aprendizagem do ambiente onde está instalado (i.e. processos e aplicações instaladas e a correr nos endpoints). Esta deverá ser utilizada na fase inicial de instalação e configuração;
c) A solução proposta deve ter a capacidade de controlar o que pode ser executado no endpoint, a partir de onde pode ser executado e com que parâmetros;
d) A solução proposta deve prevenir um processo de lançar qualquer processo legítimo que possa ser utilizado para fins maliciosos. Esta técnica é muitas vezes utilizada em ransomware e outros malwares para fazer bypass à segurança do endpoint;

e) A solução proposta deve ser capaz de bloquear processos filhos iniciados por um determinado processo através de whitelist (bloquear todos exceto os listados) e blacklist (bloquear apenas os listados);
f) A solução proposta deve ser capaz de prevenir a execução de malware através da análise de comportamentos desencadeados pelo malware;
g) A solução proposta deve garantir a possibilidade de configurar whitelists globais para permitir a execução de certos ficheiros executáveis;
h) A solução proposta deve ser capaz de criar regras de exclusão das capacidades de proteção para endpoints específicos;
i) A solução proposta deve detetar e bloquear malware através do uso de machine learning e não deve utilizar assinaturas locais independentemente do sistema operativo;
j) A solução deve ser capaz de analisar ficheiros do tipo mach-o, ELF e APK;
k) A solução proposta deve ter a opção de integrar com soluções de Advanced Persistent Threat (APT) na cloud, tendo a capacidade de fornecer uma prevenção efetiva mesmo quando não possui ligação à cloud ou ao serviço de gestão centralizado. A solução de APT na cloud deve ser do mesmo fabricante da solução proposta para garantir uma maior integração;
l) Para ficheiros desconhecidos, a solução deve fazer upload destes para um ambiente de sandboxing e gerar um veredicto e relatório detalhado. Deve ser possível fazer upload de 1.000.000 de ficheiros por dia;
m) Para ficheiros desconhecidos em sistemas operativos Linux e MAC, a plataforma deve automaticamente submetê-los para a plataforma de sandboxing e gerar um veredito e relatório detalhado sobre o comportamento do ficheiro;
n) Deve ser possível fazer upload de ficheiros para ser analisados em ambiente de sandboxing com um tamanho até 100MB.
o) A solução deve monitorizar os diferentes processos bem como as suas relações e origens (Parent processes) de forma a ser capaz de bloquear processos com comportamento malicioso.
p) A solução deve poder receber e enviar assinaturas de malware de e para NGFWs automaticamente de forma a reduzir o tempo de deteção de novos ataques no endpoint e na rede.
q) A solução deve permitir agendar malware scans para Windows, Linux e Mac.
r) A solução deve proteger contra tentativas de adulteração, incluindo modificação e/ou disable do agente.

Requisitos adicionais:

a) Conseguir prevenir de forma efetiva Exploits e Malwares quando não existe conectividade ou atualizações do servidor de gestão e/ou acesso a recursos da cloud;
b) A solução proposta deve ter a capacidade de submeter aos serviços APT na cloud ficheiros potencialmente maliciosos;
c) A solução proposta deve conseguir visualizar na plataforma de gestão centralizada os relatórios de análise do malware;
d) A solução proposta deve ter a capacidade de modificar manualmente a decisão tomada pelos serviços APT na cloud para uma hash em particular;
e) A solução proposta deve ter a capacidade de prevenir a execução de um ficheiro no caso da sua hash ser desconhecida dos serviços APT na cloud;
f) A solução proposta deve garantir a capacidade de efetuar análises estáticas (machine learning) em modo offline para Windows, Linux e macOS;
g) A solução proposta deve conseguir analisar comportamentos de ransomware antes da execução do mesmo e deve conseguir parar ataques baseados em encriptação através da análise em tempo real de atividades de encriptação;
h) A solução proposta deve conseguir que o módulo de análise de comportamentos de ransomware opere em modo de notificação ou de prevenção;
i) A solução deve poder bloquear qualquer dispositivo USB externo que se conecte a um endpoint monitorizado pela solução. Deve ser possível bloquear determinado tipo de dispositivo USB, mas permitir apenas dispositivos de um vendedor específico ou com um Serial Number específico. Deverá ser possível criar políticas apenas temporárias;
j) A solução proposta deve ter a capacidade de automaticamente criar uma regra de exclusão e um hash de exclusão a partir do relatório de ameaças detetadas, para garantir que determinado processo possa ser executado num endpoint em particular;
k) A solução proposta deve fazer stitching de alertas provenientes de 3rd parties com os alertas gerados pelo agente de endpoint;
l) A solução proposta deve fazer stitching dos logs de rede provenientes de 3rd parties com a telemetria gerada pelo agente de endpoint;
m) A solução deve automaticamente identificar máquinas sem o agente instalado através da análise de logs de Next Generation Firewalls;
n) A solução deve disponibilizar na visão de cada incidente, informação sobre a classificação de cada hash. Deve ser possível ver diretamente na interface gráfica o veredicto dos fabricantes presentes no VirusTotal;

o) A solução deve suportar e proteger os seguintes sistemas operativos:

i. Android 8, 9, 10, 11, 12, 13, 14 e 15;
ii. iOS e iPadOS 15, 16;
iii. Debian 9, 10, 11 e 12;
iv. CentOS 6, 7, 8 e 9;
v. Oracle 6, 7, 8 e 9;
vi. Red Hat 6, 7, 8 e 9;
vii. SUSE 12 e 15;
viii. Ubuntu 12, 14, 16, 18, 20, 22 e 24;
ix. macOS 10.15, 11.x, 12.x, 13 ventura, 14 sonoma e 15 sequoia;
x. Windows 7, 8, 10 e 11;
xi. Windows Server 2008R2, 2012, 2016, 2019, 2022 e 2025.

p) A solução deve suportar ainda os seguintes ambientes virtuais: Citrix XenApp, Citrix App layering, VMware AppVolumes, Vmware ThinApp;

q) No caso de não existir ligação à internet, o agente deve ser capaz de manter a cache dos dados coletados pelo módulo de EDR localmente, mesmo que seja feito um reboot.

Endpoint Detection and Response:

a) Capacidade de monitorizar continuamente toda a atividade dos endpoints, nomeadamente informação relativa a ações sobre: processos, ficheiros, tráfego de rede, registry, RPC Calls, System Calls, event logs de segurança e memória. Qualquer atividade relacionada com estes pontos deve ser guardada no mínimo para os últimos 30 dias. A solução não deve estar dependente de eventos específicos para recolher continuamente todos os dados mencionados. É obrigatório reter toda a informação independentemente da existência de incidentes de segurança;
b) Com base na informação disponível para os últimos 30 dias, a solução deve ser capaz de detetar máquinas comprometidas, seja com base em análise de processos, ficheiros, registry, e tráfego de rede nas máquinas ou com base na análise do comportamento do utilizador ligado na máquina;
c) Permitir ao analista definir regras e pesquisar por padrões relacionados com toda a informação que é retida para os endpoints. Por exemplo, deve ser possível pesquisar por endpoints onde determinada registry key foi modificada. Isto sem ser necessário utilizar ou aprender uma nova query language;

d) Quando diferentes alertas estão relacionados, a solução deve ser capaz de os agregar automaticamente em um único incidente;
e) Deve ser possível agregar diferentes incidentes num único de forma manual;
f) Deve ser possível alterar a severidade de um incidente (ex: passar de Medium para High);
g) Quando é identificado um novo incidente, a solução deve ser capaz de automaticamente identificar a root cause do incidente e mostrar toda a sequência de eventos que causou o incidente, assim como todas as alterações introduzidas por estes eventos. Para cada evento deve ser possível visualizar o processo associado, o tráfego de rede gerado por esse processo, os ficheiros acedidos alterados ou criados, qualquer modificação no registry, assim como todos os módulos/DLLs carregados por este processo em memória;
h) Para cada incidente, a solução deve indicar: todos os alertas associados a este incidente, todos os artefactos relevantes para a investigação, as máquinas e os utilizadores envolvidos. Cada incidente deve ter uma funcionalidade de chat e de notas para os analistas poderem colaborar entre si;
i) Para cada artefacto deve existir informação sobre se há assinaturas válidas para estes, assim como um veredicto sobre o artefacto da própria cloud do fabricante assim como de ferramentas OpenSource (ex: VirusTotal);
j) A solução deve mapear os diferentes alertas para a Framework Mitre ATT&CK;
k) A solução deve aprender o comportamento de cada máquina e criar perfis por endpoint de forma a ser capaz de identificar comportamentos anômalos;
l) A solução deve aprender o comportamento de cada utilizador e criar perfis por utilizador de forma a ser capaz de identificar comportamentos anômalos;
m) A solução deve identificar o perfil comportamental de todas as máquinas com e sem agente instalado;
n) Com base na aprendizagem comportamental para cada máquina e utilizador a solução deverá ser capaz de gerar automaticamente alarmística para estes cenários:

    i. Sessão rara de SSH;
    ii. Uso de comandos fora do comum (arp -a, ipconfig, etc);
    iii. Scripts raros a comunicar com hosts externos;
    iv. Enumeração de contas de domínio;
    v. Pesquisa por ficheiros locais com passwords;
    vi. Login anormal via RDP;
    vii. Comando de powershell suspeito.

o) Capacidade de reverter automaticamente alterações feitas na máquina por determinado malware. A solução deve listar as alterações feitas por qualquer processo malicioso e permitir reverter essas alterações;

p) A solução deve disponibilizar uma funcionalidade de identificação de ameaças avançada que permita a melhor cobertura para vetores de ameaças de identidade furtivos, incluindo contas comprometidas e ameaças internas;

q) Através de licenciamento adicional, a solução deverá incluir capacidades de automação nas ações de resposta de endpoint, gestão de incidentes e alertas e ações de comunicação externa (email, slack, syslog).

Network Traffic Analysis:

a) A solução deve disponibilizar um módulo de Network Traffic Analysis;
b) A solução deve utilizar as firewalls existentes no Data Center como sensores, removendo a necessidade de instalar sensores dedicados para coletar o tráfego de rede;
c) A solução deve trazer out-of-the-box mais de 100 use cases de análise comportamental especificamente desenhados para os dados coletados pelo sensor do fabricante. Estes use cases devem ser constantemente atualizados pelo fabricante;
d) A solução deve ser capaz de ingerir dados da rede do cliente (on-prem e cloud) de forma a ter visibilidade de todo o tráfego de rede e efetuar deteção comportamental sobre a rede, endpoint e cloud numa única solução e interface gráfica;
e) Deve ser possível, através de licenciamento adicional, colocar VMs a funcionar como sondas em ambientes de cloud para colectar tráfego de rede e fazer deep packet inspection, nomeadamente: AWS, Azure, GCP e Alibaba. Estas VMs deverão dispor de funcionalidades de NGFW, IPS, sandboxing, DNS Security e URL Filtering;
f) A solução proposta deve fazer stitching dos logs provenientes dos sensores na rede com os logs dos endpoints de forma a permitir a unificação dos mesmos e simplificar o processo de deteção e investigação de ameaças;
g) A solução proposta deverá utilizar Machine Learning para criar perfis das diferentes máquinas e utilizadores na rede de forma a detetar comportamentos anómalos que sejam indicadores de ataques;
h) Com base nos perfis criados a solução deverá out-of-the-box detetar automaticamente os seguintes use cases:
    i. Malware a ser transmitido na rede;

ii. Máquina com um número anormal de conexões falhadas para outros endpoints;
iii. Port Scan;
iv. Novo tipo de comportamento administrativo;
v. DNS Tunneling;
vi. Número anormal de resoluções de DNS falhados;
vii. DGA (Domain Generated Algorithm);
viii. Acesso recorrente a IP fora do comum na organização;
ix. Login anormal a um Domain Controller;
x. Tráfego para uma aplicação e destino fora do comum;
xi. Volume anormal de dados a ser transferidos.

i) A solução deve possuir analítica out-of-the-box para as seguintes fontes de dados: Amazon S3 (flow logs), Azure Event Hub, Azure Network Watcher (flow logs), Check Point FW1/VPN1, Cisco ASA, Corelight Zeek, Fortinet Fortigate, Google Cloud Platform (flow logs), Okta, Windows DHCP, Zscaler Cloud Firewall;
j) A solução deve utilizar as seguintes fontes para Identity Analytics: AzureAD, Amazon S3 (audit logs), Azure Event Hub (audit logs), Google Cloud Platform (audit logs), Microsoft Office 365, Okta, PingFederate, PingOne for Enterprise, Workday;
k) A solução deve possuir analítica para detetar anomalias ao nível dos acessos VPN através da análise dos logs dos seguintes fabricantes: Checkpoint, Paloalto e Cisco ASA;
l) O fabricante da solução de endpoint deve ter também uma solução de Next Generation Firewall que esteja presente no quadrante mágico da Gartner de network firewalls nos últimos 3 anos;
m) No caso de ser identificado um comportamento malicioso na rede, deve ser possível obter informação sobre os processos a correr na máquina afetada mesmo que esta não tenha nenhum agente instalado. Neste cenário a solução deve ter a capacidade de instalar automaticamente um agente dissolúvel para obter esta informação.

Visibilidade sobre máquinas:

A solução deve possibilitar incluir um módulo de visibilidade com as seguintes características:

a) Capacidade de identificar: Utilizadores e grupos configurados em cada máquina; Serviços a correr nas máquinas; Drivers instalados nas máquinas; Processos, drivers, serviços que são automaticamente inicializados sempre que o utilizador liga as máquinas; Shares de rede configurados nas máquinas; Discos existentes nas máquinas;

b) Funcionalidade de "search&destroy" que permita pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo;
c) Identificar vulnerabilidades e respetiva criticidade para ambientes Windows e Linux;
d) Identificar vulnerabilidade ao nível das aplicações a correr nas máquinas;
e) Identificar as aplicações instaladas em cada equipamento.

Resposta a incidentes:

a) Deve ser possível efetuar blacklist e whitelists a hashes;
b) Deve ser possível fazer quarentena a determinados processos;
c) Durante a investigação de um incidente, a solução deve permitir isolar da rede máquinas infetadas;
d) A solução deve permitir reverter automaticamente alterações que tenham sido efetuadas por um processo malicioso. Exemplo: alterar uma registry key para o valor anterior ao comprometimento da máquina;
e) Deve existir uma funcionalidade de Live Terminal, onde o analista possa aceder remotamente às máquinas de forma a: gerir os processos e ficheiros, correr scripts Python, correr comandos de Powershell e aceder à linha de comandos da máquina;
f) Deve ser possível correr scripts em python sobre todo o parque de máquinas instalado em simultâneo. A solução deve disponibilizar scripts para os use cases mais comuns e permitir a criação de novos scripts;
g) Deve ser possível correr scripts em python em ambientes Linux e MAC sem ter python instalado na máquina;
h) A solução deve ser capaz de adicionar automaticamente IPs e domínios à lista de bloqueio de uma NGFW;
i) A solução deve permitir automatizar o processo de resposta a incidentes;
j) Deve ser possível a criação de regras, para definir as ações que a plataforma deve tomar autonomamente para determinado tipo de incidente. Exemplos: Correr um script, terminar uma ligação e isolar uma máquina;
k) Capacidade de criar regras de correlação personalizadas que permitem detetar ataques retroativamente;
l) A solução deve incluir uma linguagem de consulta avançada que suporte wildcards, expressões regulares, JSON, agregação de dados, manipulação de campos e valores, agregação de dados de fontes diferentes e visualização de dados.

Funcionalidades adicionais licenciáveis:

A solução deverá ter a capacidade de, no futuro, suportar as seguintes funcionalidades de segurança através de licenciamento adicional:

a) Forense:

i. Identificar a atividade do atacante através da revisão dos principais artefactos obtidos do endpoint, como logs de eventos, chaves de registo, histórico do browser, etc;

ii. Obter informação detalhada do sistema como lista completa de ficheiros de todas as drives, incluindo drives removidas;

iii. Permitir o download de um snapshot forense completo do endpoint, e o upload do mesmo para a solução para análise;

iv. Recolha de dados:

- Histórico do browser: Chrome; Edge; Firefox; Internet Explorer;
- Acesso a ficheiros: Recent files (LNK files); Jump lists; OpenSavePidlMRU; ShellBags; WordWheelQuery;
- Processos executados: Amcache; Application Resource Usage (SRUM); Background Activity Monitor; CIDSizeMRU; LastVisitedPidlMRU; Prefetch; RecentFileCache; Shimcache; UserAssist; Windows Timeline;
- Atividade de rede: ARP cache; DNS cache; Hosts File; Network Connectivity Usage (SRUM); Network Data Usage (SRUM);
- Acessos remotos: LogMeIn; TeamViewer;
- Histórico de comandos: PSReadLine;
- Triagem: File listing ($MFT); Registry listing; Event logs; Net sessions; Handle listing.

1.4. Serviços Profissionais

1.4.1. Migração:

O adjudicatário deverá incluir na sua proposta os serviços necessários para efetuar a migração dos atuais sistemas para aqueles propostos. Deverá ser efetuada uma análise exaustiva e migração completa das configurações existentes nos atuais equipamentos e software para os novos equipamentos e software, respetivamente.

1.4.2. Instalação:

O adjudicatário deverá assegurar os serviços profissionais e certificados para a instalação e configuração de toda a solução proposta.

O concorrente deverá incluir na sua proposta os comprovativos das certificações técnicas dos recursos humanos afetos ao projeto, de todas as componentes (hardware e software) propostos, atualizadas até à data de envio da proposta.

Sendo objetivo dos SMASTV a contratação de uma solução "chave-na-mão", o adjudicatário deverá providenciar todos os meios para a concretização deste fim.

1.4.3. Testes e aceitação:

A adequação do resultado do fornecimento da solução, efetuada face aos requisitos estabelecidos e à documentação técnica facultada, será aferida através da realização de testes, que serão definidos pelo serviço IT dos SMASTV, com a colaboração da entidade adjudicatária.

Os testes deverão ser realizados no prazo máximo de 10 dias úteis a contar da conclusão da instalação da solução.

1.5. <u>Formação</u>

A formação da solução a implementar deve encontrar-se incluída na proposta. Deve ser garantida pelo adjudicatário, formação certificada à equipa de gestão e operação da rede, composta por pelo menos 3 elementos, com o equivalente de 8 horas nas instalações dos SMASTV.

Cláusula 18.ª

Prazos dos serviços de manutenção e garantia

Todos os equipamentos e software da solução proposta deverão ter garantia com manutenção preventiva e corretiva por um período mínimo de 3 anos.

O nível de serviço e tempos de resposta para a manutenção deverá ser de acordo com a seguinte informação:

a) Suporte disponível de segunda a sexta-feira, 8 horas por dia, excluindo feriados, com tempo de resposta on-site no dia útil seguinte;
b) Diagnóstico e resolução de problemas com assistência on-site;
c) Tempo de reposição on-site: dia útil seguinte;

d) Fornecimento de peças de reposição: dia útil seguinte.

Todas as intervenções realizadas ao abrigo da garantia ou serviço de manutenção deverão ser concluídas com a entrega de um relatório de intervenção.

Cláusula 19.ª

Prazos de disponibilização

Os prazos máximos de disponibilização a considerar, após a data da última assinatura do contrato, serão os seguintes:

- Para o licenciamento – máximo de 3 (três) dias;
- Para o hardware – máximo de 30 (trinta) dias.

Cláusula 20.ª

Requisitos de sustentabilidade

A solução deverá garantir a integração com solução de terceiros, permitindo a compatibilidade com infraestruturas existentes e facilitando a reutilização de tecnologias e dispositivos já implementados. Evitando assim, bloqueios tecnológicos, promovendo a flexibilidade e a interoperabilidade com outros sistemas, permitindo ainda expansões e atualizações graduais sem necessidade de substituições.

Anexo A

CÓDIGO DE CONDUTA PARA AS ENTIDADES FORNECEDORAS

1. APRESENTAÇÃO

Nos SMASTV – Serviços Municipalizados de Água e Saneamento da Câmara Municipal de Torres Vedras, doravante designados por SMASTV, pautamos a nossa atividade com vista a garantir a gestão eficiente dos serviços prestados (abastecimento de água, drenagem de águas residuais e recolha de resíduos urbanos), com vista à satisfação do/a cliente, promovendo o desenvolvimento sustentável – ambiental, económico e social – e a segurança de todos/as.

Assumimos a convicção de que, para assegurar o cumprimento da nossa missão, devemos estabelecer/reforçar os laços de confiança com os/as nossos/as clientes, trabalhadores/as, fornecedores/as e a comunidade, pautando a nossa atuação com base no respeito pela legalidade e igualdade de tratamento.

Com esse propósito, elaborou-se o presente código, no qual apresentamos os valores, princípios e conduta que alicerçam a cultura organizacional dos SMASTV e que gostaríamos que os/as nossos/as fornecedores/as adotassem nos compromissos assumidos com os SMASTV.

Através da aceitação deste documento, os/as nossos/as Fornecedores/as e seus Subcontratados/as expressam e assumem o compromisso em cumprir o Código, adotando comportamentos transparentes nos seus relacionamentos com os SMASTV, Clientes e outras Partes Interessadas, através da **adoção de padrões éticos e da criação de um ambiente de trabalho que assegure a qualidade e promova a segurança e saúde no trabalho, o respeito, a integridade, a igualdade de tratamento, a proteção e preservação do ambiente, a segurança da informação dos SMASTV e das suas Partes Interessadas**, complementando as obrigações e os compromissos decorrentes de disposições legais, regulamentares, normativas e contratuais.

O presente documento encontra-se disponível no sítio dos SMASTV **(https://www.smastv.pt)**, na área de Fornecedores, estando em permanente atualização.

2. ÂMBITO DE APLICAÇÃO

O Código aplica-se a todos/as os/as entidades fornecedoras e subcontratados/as (de bens, serviços e empreitadas), dos SMASTV, adiante designados/as como fornecedores/as.

A aceitação e o cumprimento do disposto neste Código, que constitui uma obrigação contratual, prevê que o/a fornecedor/a proceda à sua **divulgação** entre os/as seus/as trabalhadores/as e subcontratados/as, quando aplicável, bem como assegure o seu cumprimento, nas ações quotidianas por parte das pessoas envolvidas.

Os SMASTV esperam que os/as seus/as fornecedores/as desenvolvam políticas e procedimentos no sentido de promover níveis de exigência equivalentes aos que constituem este Código de Conduta junto das suas cadeias de fornecimento.

3. REFERENCIAIS DE CONDUTA DOS SMASTV

Com uma atividade ligada à valorização e proteção do ambiente, à melhoria da saúde pública e do bem-estar humano e ao progresso da sociedade a nível ambiental, estamos comprometidos com o desenvolvimento sustentável, tendo como prioridade garantir o fornecimento de água para consumo humano, de qualidade, e o adequado tratamento de águas residuais,

bem como o encaminhamento dos resíduos sólidos urbanos para destino final apropriado, de acordo com as normas legais.

Os compromissos que exigimos aos/às nossos/as fornecedores/as, advêm das normas legais em vigor, aplicáveis no âmbito da contratação pública, e dos referenciais subscritos pelos SMASTV e seguidos no âmbito do desenvolvimento da sua atividade e que passamos a identificar:

- Pacto Institucional para a Valorização da Economia Circular na Região Centro (CCDRC);
- Plano de prevenção de riscos de corrupção e infrações conexas (PPRCIC), no âmbito da Estratégia Nacional Anticorrupção.

4. DIRETRIZES PARA FORNECEDORES/AS

Esta secção descreve os compromissos assumidos por todos/as os/as fornecedores/a, no sentido de contribuir para a sua melhor integração no ambiente de trabalho, no desenvolvimento das suas funções e atividades e na relação e contacto com as partes interessadas internas e externas da organização, designadamente trabalhadores/as e clientes.

Assim, o agente económico e, sendo o caso, os/as seus/suas trabalhadores/as e subcontratados/as devem:

COMPROMISSO DE COMPLIANCE

DA CONFORMIDADE LEGAL

- Respeitar todas as normas legais e regulamentares aplicáveis à sua atividade, ao fornecimento de bens e serviços e à execução de empreitadas de obras públicas.
- Respeitar e garantir a conformidade com toda a legislação, regulamentação e normas em vigor, aplicáveis ao fornecimento de bens e serviços, à execução de empreitadas de obras públicas e à relação contratual estabelecida com os SMASTV.
- Cumprir com as obrigações assumidas perante os SMASTV, em virtude da celebração de quaisquer contratos.

COMPROMISSO COM OS DIREITOS FUNDAMENTAIS

DO RESPEITO E PROTEÇÃO DOS DIREITOS

- Respeitar a legislação internacional, europeia e portuguesa, em matéria de direitos fundamentais, direitos laborais, proteção dos dados pessoais, segurança e saúde, preservação e

proteção do ambiente, transparência, conduta ética e respeito pela vida privada e familiar dos/as trabalhadores/as.

- Adotar políticas internas de promoção e respeito dos direitos humanos, nomeadamente igualdade de tratamento e não discriminação, fundada na raça, sexo, idade, condição física, ou qualquer outro fator.
- Não utilizar e/ou tolerar a utilização de qualquer forma de exploração e trabalho infantil, devendo respeitar a idade mínima de admissão prevista na legislação em vigor.
- Tratar os/as trabalhadores/as com dignidade e respeito.
- Respeitar e cumprir as disposições legais e regulamentares em vigor em matéria de direito do trabalho e de segurança e saúde no trabalho.

DO RESPEITO E PROTEÇÃO DOS DIREITOS DOS/AS TRABALHADORES/AS

- Garantir a remuneração adequada aos/às trabalhadores/as e respeitar o limite máximo de horas de trabalho, normal e suplementar, bem como os períodos e dias de descanso, em conformidade com a legislação em vigor.
- Garantir trabalho decente para todas as mulheres e homens, inclusive para os jovens e pessoas com deficiência.
- Assegurar que a retribuição mensal de todos/as os/as seus/suas trabalhadores/as seja igual, para trabalho de igual valor.
- Promover um ambiente de trabalho seguro e protegido para todos/as trabalhadores/as, incluindo os/as trabalhadores/as migrantes, em particular as mulheres migrantes.
- Respeitar a liberdade de associação e negociação coletiva dos/as seus/suas trabalhadores/as, abstendo-se de qualquer tipo de julgamento, represália ou discriminação.
- Promover a formação dos/as seus/suas trabalhadores/as de forma a melhorar as suas capacidades laborais e a contribuir para práticas sustentáveis.
- Adotar medidas que promovam a conciliação da vida profissional, familiar e pessoal dos /as seus/suas trabalhadores/as.

COMPROMISSOS DE GESTÃO

DA ÉTICA E CONDUTA

- Garantir o respeito pela propriedade intelectual.
- Prevenir a ocorrência de situações ou de comportamentos que prejudiquem ou possam pôr em causa a imagem, a reputação e o prestígio dos SMASTV ou a privacidade dos demais.
- Conhecer e atuar em conformidade com o Código de Ética e Boa Conduta dos SMASTV.

DA RESPONSABILIDADE

- Desenvolver a consciência ambiental e de responsabilidade social.
- Adotar práticas que promovam o desenvolvimento sustentável.
- Dar a conhecer, aos SMASTV, toda a informação de que tenha conhecimento superveniente à data da celebração do contrato e que seja relevante para a boa execução do contrato.
- Respeitar os compromissos assumidos pelos SMASTV para com os/as seus/as clientes, sempre que atuem para e em nome dos SMASTV, em virtude dos contratos celebrados.
- Abster-se de fornecer informações a terceiros alheios ao contrato, sobre os SMASTV, exceto quando autorizados pelos SMASTV para o efeito.
- Responsabilizar-se por quaisquer danos causados, pelos/as seus/as trabalhadores/as e subcontratados/as, no exercício das respetivas funções e atividades contratadas.
- Utilizar as marcas, logotipos e demais material fornecido pelos SMASTV, em conformidade com o acordado com estes SMASTV, devolvendo-o assim que cesse o contrato ou mediante solicitação.

DA GESTÃO DA CADEIA DE ABASTECIMENTO

- Assegurar que os/as parceiros/as selecionados/as pelos/as fornecedores/as assumam os mesmos compromissos por estes/as assumidos, no que concerne à prestação de serviços, fornecimento de bens ou à execução de empreitadas de obras públicas.
- Garantir que as matérias-primas, materiais e produtos utilizados na realização das prestações acima referidas, cumprem os requisitos

legais aplicáveis e estão de acordo com os regulamentos internacionais, europeus ou nacionais.

- Assegurar a existência de mecanismos de acompanhamento da conformidade legal dos/as seus/as parceiros/as, subcontratados/as e prestadores de serviços.

DA CONFIDENCIALIDADE E SIGILO PROFISSIONAL

- Garantir - e assegurar que todos/as os/as seus/as trabalhadores/as e subcontratados/as assegurem - a confidencialidade e o sigilo profissional sobre toda a informação e documentação relativa aos SMASTV, bem como sobre toda a informação privada, de que possam ter conhecimento ao abrigo ou relacionada com a execução do contrato, garantindo:

  a) A não transmissão a terceiros;

  b) O respeito entre as partes envolvidas.

- Garantir que todos/as os/as seus/as representantes e colaboradores/as e demais pessoas por si autorizadas a tratar dados pessoais se vinculam validamente, através de um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade.

DA PREVENÇÃO DA CORRUPÇÃO

- Adotar práticas transparentes que evitem conflitos de interesses.

- Implementar medidas com vista a impedir a ocorrência de qualquer prática ou conduta suscetível de configurar um ato de corrupção ou tráfico de influências, punível criminalmente ao abrigo da legislação aplicável.

DO RESPEITO E PROMOÇÃO DA IGUALDADE DE GÉNERO E DE OPORTUNIDADES

- Respeitar a igualdade de género e promover a não discriminação.

- Valorizar os/as trabalhadores/as com base no seu mérito, capacidade e empenho.

- Garantir a igualdade de oportunidades e de tratamento na admissão, no desenvolvimento da carreira, no acesso à formação e na política remuneratória.

DA ERRADICAÇÃO DE TODAS AS FORMAS DE EXPLORAÇÃO

- Não utilizar e/ou tolerar o recurso a trabalho forçado, o recurso a trabalhadores/as ilegais, e condenar quaisquer práticas ilegais que obriguem os/as trabalhadores/as à execução do trabalho.
- Não adotar ou permitir comportamentos abusivos ou qualquer tipo de punição física ou mental, que possam configurar coação, nas suas vertentes de assédio moral ou sexual, práticas de *bullying*, humilhação ou de ameaça.

DA PROMOÇÃO DA SEGURANÇA, SAÚDE E BEM-ESTAR

- Respeitar a legislação portuguesa, os princípios e as recomendações das Organizações Governamentais nacionais, europeias e internacionais em matéria de segurança, saúde e bem-estar no trabalho.
- Promover condições de trabalho seguras e benéficas ao bem-estar físico, mental e emocional.
- Implementar medidas para prevenir e mitigar os riscos associados às atividades desenvolvidas, providenciando os recursos necessários para o efeito.
- Assegurar formação regular sobre segurança no trabalho.
- Disponibilizar equipamentos de proteção, adequados à execução das atividades contratadas, bem como, de equipamentos de trabalho em bom estado de segurança e conservação.
- Adotar medidas que combatam a utilização de estupefacientes ou substâncias psicotrópicas e álcool durante o período de trabalho por parte dos/as trabalhadores/as.

DA SEGURANÇA DA INFORMAÇÃO

- Salvaguardar a confidencialidade, integridade e disponibilidade da informação de acordo com sistemas adequados de segurança.
- Adotar as medidas de segurança necessárias para garantir a integridade e bom funcionamento dos sistemas de informação.
- Respeitar e cumprir o disposto no Regulamento Geral de Proteção de Dados, nomeadamente aceder e tratar os dados pessoais a que tiver acesso, somente para a finalidade que lhe foi solicitada pelos SMASTV e que

é objeto do contrato, assim como adotar as medidas necessárias e adequadas para garantir a segurança da informação, como preconizado no clausulado contratual.

COMPROMISSOS COM O AMBIENTE E O DESENVOLVIMENTO SUSTENTÁVEL

DA PROMOÇÃO, DA PRESERVAÇÃO E PROTEÇÃO DO AMBIENTE

- Respeitar a legislação portuguesa, os princípios e as recomendações das Organizações Governamentais nacionais, europeias e internacionais em matéria de ambiente.
- Contribuir para o desenvolvimento sustentável e para a preservação e proteção ambiental.
- Implementar medidas para reduzir os riscos e os impactes ambientais negativos das suas atividades, produtos e materiais utilizados.
- Promover a racionalização da utilização e consumo dos recursos naturais e a redução das emissões e resíduos originados pelas suas atividades e fornecimento de bens e/ou serviços.
- Implementar medidas para melhorar o desempenho e a eficiência energética, associadas às suas atividades e ao fornecimento de bens e/ou serviços.
- Adotar medidas e práticas no âmbito da economia verde e da economia circular.
- Contribuir para o progresso e bem-estar das comunidades, melhorando a qualidade de vida dos/as cidadãos/as, contribuindo para o desenvolvimento socioeconómico e proteção ambiental.
- Adotar medidas que contribuam para o cumprimento das metas dos ODS – Objetivos de Desenvolvimento Sustentável, em particular, reduzir substancialmente a produção de resíduos através da prevenção, redução, reciclagem e reutilização.
- Usar, de forma eficiente e correta, os recursos dos SMASTV – no caso dos contratos preverem esta situação – com vista à prossecução dos objetivos definidos, devendo as pessoas zelar pela proteção, integridade e bom estado de conservação dos mesmos.

5. APLICAÇÃO DO CÓDIGO

Os SMASTV estão a desenvolver mecanismos de acompanhamento dos compromissos e do desempenho dos/as seus/as fornecedores/as para a sua implementação progressiva.

Qualquer dúvida na interpretação deste documento deverá ser remetida, por escrito, antes do início do fornecimento de bens, serviços ou da execução da empreitada de obras públicas aos SMASTV ou no período de execução do contrato ao/à Gestor/a de Contrato designado/a pelos SMASTV.

Poderá constituir motivo de reclamação dos SMASTV, a violação por parte dos/as fornecedores/as dos compromissos e requisitos que constituem o presente Código de Conduta.

Com os valores, princípios e conduta que alicerçam a cultura organizacional dos SMASTV e que constam do presente código, os SMASTV contribuem para os seguintes Objetivos de Desenvolvimento Sustentável: