



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

CADERNO DE ENCARGOS

Fornecimento, instalação e suporte da plataforma Azores Cyber 360º



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

ÍNDICE

CLÁUSULAS JURÍDICAS	4
Cláusula 1.ª Objeto	4
Cláusula 2.ª Contrato	4
Cláusula 3.ª Local da entrega e instalação dos bens	5
Cláusula 4.ª Preço base.....	5
Cláusula 5.ª Duração do contrato.....	5
Cláusula 6.ª Obrigações principais do cocontratante.....	5
Cláusula 7.ª Condições de pagamento	6
Cláusula 8.ª Direitos de propriedade intelectual e industrial.....	6
Cláusula 9.ª Sigilo.....	7
Cláusula 10.ª Proteção de dados pessoais	8
Cláusula 11.ª Cessão da posição contratual	8
Cláusula 12.ª Deveres de colaboração recíproca e informação	8
Cláusula 13.ª Seguros	8
Cláusula 14.ª Força maior	9
Cláusula 15.ª Foro competente	10
Cláusula 16.ª Legislação aplicável.....	10
CLÁUSULAS TÉCNICAS	11
Cláusula 17.ª Especificações técnicas	11
Cláusula 18.ª Conformidade e operacionalidade dos bens	11
Cláusula 19.ª Prazos de entrega	11
Cláusula 20.ª Condições de entrega	12
Cláusula 21.ª Verificação e aceitação dos bens.....	12
Cláusula 22.ª Garantia dos bens	13
Cláusula 23.ª Entregáveis e documentação	15
Cláusula 24.ª Formação	15
Cláusula 25.ª Planeamento.....	15



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Cláusula 26. ^a Mecanismos formais de acompanhamento	16
Cláusula 27. ^a Sanções	17
ANEXO A – REQUISITOS FUNCIONAIS E TÉCNICOS	18
1 Enquadramento.....	18
2 Caracterização da situação atual.....	18
3 Solução tecnológica pretendida	19
4 Segurança dos endpoints	21
5 SIEM (<i>Security information and event management</i>)	27
6 Análise de tráfego	29
7 SOAR (<i>Security Orchestration Automation and Response</i>)	32
8 Gestão de vulnerabilidades	41
9 Serviços de implementação	43
10 Condições de assistência na garantia.....	50
11 Níveis de serviço	51
12 Aplicação das sanções	53
13 Organização e metodologia de execução.....	55
14 Qualificações e experiência do pessoal técnico	55
15 Estrutura da proposta técnica	56
ANEXO B – MATRIZ DE RESPOSTA A PONTO POR PONTO	58



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

- 1 - O contrato a celebrar tem como objeto o fornecimento, instalação e suporte da plataforma Azores Cyber 360º, nos termos definidos nas cláusulas técnicas do presente Caderno de Encargos.
- 2 - O fornecimento objeto do contrato a celebrar compreende também os serviços acessórios de transporte, montagem, instalação, configuração e teste da solução, bem como os serviços de garantia e suporte, nos termos definidos no Anexo A deste Caderno de Encargos.
- 3 - A aquisição de bens tem o Código CPV (Common Procurement Vocabulary) nº 48000000-8.

Cláusula 2.ª

Contrato

- 1 - O contrato a celebrar integra, para além do respetivo clausulado e seus anexos, os seguintes elementos:
 - a) Os suprimentos dos erros e, das omissões do Caderno de Encargos identificados pelos interessados, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c) O presente Caderno de Encargos;
 - d) A proposta adjudicada;
 - e) Os esclarecimentos sobre a proposta adjudicada prestados pelo prestador dos serviços.
- 2 - Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.
- 3 - Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos e aceites pelo prestador dos serviços nos termos do disposto no artigo 101.º desse mesmo diploma legal.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Cláusula 3.ª

Local da entrega e instalação dos bens

- 1 - A solução deverá ser entregue e instalada nos Centros de Dados da entidade adjudicante, localizados nas Ilhas de São Miguel e Terceira, cujas moradas serão disponibilizadas ao adjudicatário, após a celebração do contrato.
- 2 - Todas as despesas relativas a transportes, deslocações e alojamento estão incluídas no preço constante da proposta.

Cláusula 4.ª

Preço base

- 1 - O preço base é de € 1.670.000,00 (Um milhão, seiscentos e setenta mil euros).
- 2 - São excluídas as propostas cujo valor seja superior ao preço base.

Cláusula 5.ª

Duração do contrato

O contrato terá a duração de 150 dias contados da data de conclusão do processo de visto do Tribunal de Contas (n.º 1 do artigo 48.º da Lei de Organização e Processo do Tribunal de Contas, aprovada pela Lei n.º 98/97, de 26 de agosto), e sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 6.ª

Obrigações principais do cocontratante

- 1 - Sem prejuízo de outras obrigações previstas na legislação aplicável, no Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorre para o cocontratante a obrigação principal de:
 - a) Entrega da solução adjudicada (hardware, software, serviços e documentação) plenamente operacional, nos termos do Anexo A deste Caderno de Encargos;
 - b) Garantia;
 - c) Suporte ao software e *firmware*.
- 2 - Comunicar, por escrito, a conclusão da entrega e instalação da solução logo quando ocorra.
- 3 - O cocontratante é responsável por qualquer defeito ou não conformidade com as características, especificações e requisitos estabelecidos no contrato.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 4 - O adjudicatário compromete-se a fornecer todos os detalhes adicionais e esclarecimentos, relativos à solução implementada, e em tempo útil, que venham posteriormente a ser solicitados pelo Governo Regional dos Açores, mesmo após a cessação da vigência do contrato.
- 5 - É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a eles relativas, no que respeita à conformidade dos bens.

Cláusula 7.ª
Condições de pagamento

- 1 - A faturação é efetuada nos seguintes termos:
 - a) 75 % após a entrega dos bens objeto do presente procedimento;
 - b) 20% após a aceitação provisória dos bens, nos termos do número um da Cláusula 21ª deste Caderno de Encargos;
 - c) 5% após a aceitação definitiva dos bens, nos termos do número três da Cláusula 21ª deste Caderno de Encargos.
- 2 - O pagamento será efetuado no prazo máximo de 60 dias a contar da data da receção das faturas correspondentes, as quais só podem ser emitidas após o vencimento da obrigação a que se referem.
- 3 - Nos termos da Lei n.º 8/2012, de 21 de fevereiro, a Entidade Adjudicante emite um número de compromisso válido e sequencial, que o cocontratante deverá indicar nas faturas.
- 4 - Desde que devidamente emitidas e observado o disposto na presente cláusula, as faturas são pagas através de transferência bancária, para o NIB a indicar pelo cocontratante.
- 5 - O cocontratante não pode efetuar a transmissão de créditos ao abrigo de contratos de factoring ou proceder à cessão de créditos, sem autorização prévia do Contraente Público.

Cláusula 8.ª
Direitos de propriedade intelectual e industrial

- 1 - São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.
- 2 - O cocontratante entregará à Entidade Adjudicante no termo do contrato toda a documentação e desenvolvimento, relativo aos trabalhos realizados especificamente para a entidade adjudicante, incluindo as respetivas fontes que serão propriedade da Entidade Adjudicante.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 3 - A Entidade Adjudicante poderá transformar e reproduzir todos os documentos e todo o software desenvolvido, nos termos do número anterior, bem como proceder à sua distribuição, onerosa ou gratuita, de forma inteiramente livre.
- 4 - Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente Caderno de Encargos.
- 5 - Se a Entidade Adjudicante vier a ser demandada por ter sido infringido, na execução do contrato, qualquer dos direitos mencionados no presente artigo, o cocontratante responderá nos termos do disposto no artigo 447.º, n.º 2, do Código dos Contratos Públicos.

Cláusula 9.ª

Sigilo

- 1 - O cocontratante obriga-se a observar sigilo quanto a informação e documentação, técnica e não técnica, comercial ou outra, relacionada com a atividade da Entidade Adjudicante ou qualquer outra entidade envolvida na execução do contrato.
- 2 - A informação e documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
- 3 - O cocontratante obriga-se ainda a respeitar a confidencialidade sobre todos os dados ou informações de carácter funcional ou processual dos serviços da Administração Pública a que tenha acesso na execução do contrato.
- 4 - O cocontratante assume igualmente o compromisso de remover e destruir, no final do contrato, todo e qualquer registo, eletrónico ou em papel, relacionado com os dados e processos analisados e que a Entidade Adjudicante lhe indique para esse efeito.
- 5 - O cocontratante obriga-se, de um modo especial, a guardar sigilo quanto ao conteúdo e utilização dos sistemas de informação da responsabilidade da Entidade Adjudicante, nos termos legalmente previstos na Lei n.º 58/2019, de 8 de agosto.
- 6 - O cocontratante garante que terceiros que envolva na execução dos serviços respeitem as obrigações de sigilo e confidencialidade constantes nos números anteriores.
- 7 - confidencialidade constantes nos números anteriores.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Cláusula 10.ª

Proteção de dados pessoais

- 1 - O Cocontratante garante o cumprimento do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, designadamente o disposto no artigo 28.º, bem como legislação complementar aplicável.
- 2 - Quando solicitado, o Cocontratante obriga-se a apresentar ao Contraente Público, no prazo de 48 horas, as medidas adotadas que evidenciam o cumprimento as disposições relativas à proteção de dados pessoais.

Cláusula 11.ª

Cessão da posição contratual

O cocontratante não pode ceder a sua posição no contrato sem autorização prévia do Contraente Público.

Cláusula 12.ª

Deveres de colaboração recíproca e informação

As partes estão vinculadas pelo dever de colaboração mútua, designadamente no tocante à prestação recíproca de informações necessárias à boa execução do contrato, sem prejuízo dos deveres de informação previstos no artigo 290.º do CCP.

Cláusula 13.ª

Seguros

- 1 - É da responsabilidade do Cocontratante a cobertura, através de contratos de seguro de responsabilidade civil extracontratual destinados a garantir o ressarcimento dos danos causados a terceiros por atos ou omissões negligentes, nos termos da legislação em vigor, e de riscos de acidentes de trabalho e doenças profissionais, devendo nas apólices constar uma cláusula pela qual a entidade se compromete a mantê-las válidas até à conclusão da prestação de serviços.
- 2 - O Contraente Público pode, sempre que entender conveniente, exigir prova documental da celebração dos contratos de seguro referidos no número anterior, à exceção dos que foram exigidos nos documentos de habilitação, devendo o Cocontratante fornecê-la no prazo 5 (cinco) dias.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 3 - As condições estabelecidas nos números anteriores abrangem igualmente a atividade dos empregados, assalariados, mandatários ou pessoas diretamente envolvidas na atividade do segurado quando ao serviço deste e desde que sobre elas recaia também a obrigação de indemnização, bem como os eventuais trabalhadores ou colaboradores que venham a ser agregados, mesmo que em tempo restrito, respondendo o Cocontratante perante a Contraente Público pela sua observância.
- 4 - Os encargos referentes aos seguros impostos por este Caderno de Encargos, bem como qualquer dedução efetuada pela seguradora a título de franquia em caso de sinistro indemnizável, correm por conta do Cocontratante.

Cláusula 14.^a

Força maior

- 1 - Não é havido 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 alheias à vontade das partes, que impossibilitem a respetiva realização, desde que não se pudessem conhecer ou prever à data da celebração do contrato e cujos efeitos não fosse razoavelmente exigível contornar ou evitar.
- 2 - Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
- 3 - Não constituem força maior, designadamente:
- a) Circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do prestador de serviços ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros.
- 4 - A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
- 5 - A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas, pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 15.ª

Foro competente

Para a resolução de todos os litígios relativos, designadamente, à interpretação, execução, incumprimento, invalidade, resolução ou redução do contrato é competente o Tribunal Administrativo de Ponta Delgada.

Cláusula 16.ª

Legislação aplicável

Em tudo o omissso neste Caderno de Encargos, observar-se-á o previsto no Regime Jurídico dos Contratos Públicos da Região Autónoma dos Açores, no Código dos Contratos Públicos e demais legislação aplicável.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

CLÁUSULAS TÉCNICAS

Cláusula 17.^a

Especificações técnicas

As especificações técnicas dos bens e respetivas quantidades, encontram-se descritas no Anexo A do presente Caderno de Encargos.

Cláusula 18.^a

Conformidade e operacionalidade dos bens

- 1 - O cocontratante obriga-se a entregar à Entidade Adjudicante os bens objeto do contrato nas quantidades requeridas e com os requisitos técnicos e funcionais previstos no presente Caderno de Encargos.
- 2 - Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.
- 3 - O cocontratante é responsável perante a Entidade Adjudicante por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

Cláusula 19.^a

Prazos de entrega

- 1 - O cocontratante obriga-se a entregar, instalar e configurar os bens cuja aquisição é objeto do presente Caderno de Encargos, nos locais indicados pela Entidade Adjudicante, no prazo máximo de 150 dias, contados da data de início da vigência do contrato.
- 2 - Sempre que ocorra um caso de força maior, devidamente comprovado e que implique a suspensão da entrega, deve o cocontratante, logo que dele tenha conhecimento, requerer à Entidade Adjudicante que lhes seja concedida uma prorrogação do respetivo prazo, fundamentando adequadamente o pedido.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Cláusula 20.ª

Condições de entrega

- 1 - O cocontratante deverá comunicar previamente a data de entrega e as condições necessárias à instalação física dos bens, em condições normais de uso, com vista a garantir o perfeito funcionamento dos mesmos.
- 2 - Todas as despesas e custos com o transporte dos bens objeto do contrato e respetivos documentos para o local de entrega bem como a respetiva montagem, instalação, configuração e testes são da responsabilidade do cocontratante.
- 3 - Os riscos na fase de transporte, de acondicionamento, da embalagem, da carga e da descarga, da entrega, são da exclusiva responsabilidade do cocontratante, sem quaisquer encargos adicionais para a Entidade Adjudicante.
- 4 - Os bens deverão incorporar todas as peças e ser acompanhadas do certificado de garantia, dos manuais, das instruções técnicas e outros elementos necessários a garantir o seu funcionamento em condições normais de uso e que estão incluídas no respetivo preço.
- 5 - As embalagens dos bens devem ser conservadas fechadas e seladas pelo cocontratante até à instalação dos mesmos em condições normais de uso.
- 6 - Após a instalação, as embalagens ficarão na posse da Entidade Adjudicante e devem conter etiquetagem com as referências do cocontratante, do fabricante, da marca, do modelo, do lote de fabrico/ano, do número de série, e de todas as indicações necessárias à sua segurança.

Cláusula 21.ª

Verificação e aceitação dos bens

- 1 - Efetuada a montagem, instalação, configuração e testes dos bens nos termos previstos, bem como prestados os serviços especificados na secção 9 do Anexo A deste Caderno de Encargos, a Entidade Adjudicante, por si ou através de terceiro designado para o efeito, procede à sua inspeção quantitativa e qualitativa, com vista a verificar, respetivamente, se os mesmos correspondem às quantidades estabelecidas no contrato e se reúnem os requisitos técnicos e



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

funcionais definidos nas cláusulas técnicas (incluindo o Anexo A) do presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.

- 2 - Durante a fase de inspeção dos bens objeto do contrato, o cocontratante deve prestar toda a cooperação e todos os esclarecimentos necessários.
- 3 - Em caso de silêncio da Entidade Adjudicante, findo o prazo de 4 semanas após a entrega dos bens e dos serviços que lhe são conexos, os entregáveis consideram-se aceites provisoriamente.
- 4 - Em caso de silêncio da Entidade Adjudicante, findo o prazo de 2 semanas após a aceitação provisória, os bens consideram-se aceites definitivamente, ocorrendo a transferência da posse e da propriedade dos mesmos, sem prejuízo das obrigações de garantia e suporte que impendem sobre o cocontratante.
- 5 - No caso de a inspeção referida no n.º 1 não comprovar a conformidade dos bens, a Entidade Adjudicante informa, por escrito, o cocontratante.
- 6 - No caso previsto no número anterior, o cocontratante deve proceder, à sua custa e no prazo referido nos números seguintes, às reparações ou substituições necessárias para garantir a operacionalidade dos bens e o cumprimento das exigências legais e dos requisitos técnicos e funcionais exigíveis.
- 7 - O cocontratante dispõe de um prazo máximo de cinco dias úteis, a contar da comunicação referida no n.º 5 - , para proceder à substituição dos bens em caso de rejeição dos mesmos ou para suprir as deficiências e irregularidades detetadas durante a entrega e que não impliquem a rejeição dos bens.
- 8 - Após a realização das reparações ou substituições necessárias pelo cocontratante, no prazo respetivo, a Entidade Adjudicante procede à realização de nova inspeção, nos termos dos números anteriores.

Cláusula 22.ª
Garantia dos bens

- 1 - No que se refere aos bens entregues em execução do contrato, o cocontratante fica sujeito às exigências legais de conformidade e garantia técnica, bem como demais obrigações de fornecedor, nos prazos aplicáveis aos contratos de aquisição de bens móveis, nos termos do Código dos Contratos Públicos e demais legislação aplicável.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 2 - A aquisição de bens objeto do presente Caderno de Encargos contempla uma garantia com os níveis de serviço referidos nas cláusulas técnicas do presente Caderno de Encargos, e nos números seguintes.
- 3 - Todos os bens estão sujeitos a garantia, com a duração de 3 anos a contar da aceitação definitiva da totalidade do fornecimento contratado.
- 4 - Considera-se incluído na garantia dos bens:
 - a) As operações de natureza preventiva, designadamente, revisões, afinações, limpezas e testes necessários à redução dos riscos de avaria dos bens, de forma a garantir, em tempo, a manutenção das respetivas características a um nível semelhante às iniciais;
 - b) As operações de natureza corretiva, que têm como objetivo repor os produtos em condições normais de funcionamento sempre que ocorram falhas, avarias ou inconformidades da solução e das condições de serviço com os requisitos do presente Caderno de Encargos;
 - c) O fornecimento e substituição de peças ou outros materiais por peças ou elementos de origem, necessárias ao funcionamento dos equipamentos em condições normais de uso;
 - d) A reinstalação em condições normais de uso, no caso de transporte, dos bens avariados;
 - e) A substituição dos bens no caso de avaria não reparável;
 - f) Os custos de mão-de-obra e restantes encargos com pessoal, incluindo o transporte, para efeito das prestações previstas nas alíneas anteriores;
 - g) Todos os encargos com o transporte do material necessário à execução das prestações previstas nas alíneas anteriores.
 - h) Defeitos de fabrico/desenvolvimento em hardware ou software;
 - i) Deficiências em parametrizações e entregáveis materiais ou imateriais produzidos pelo adjudicatário;
 - j) As correções de situações de degradação dos níveis de desempenho de quaisquer componentes da solução, que violem as especificações técnicas deste Caderno de Encargos, ou afetem negativamente o seu regime normal de funcionamento, cuja origem não resulte de fatores externos à própria solução.
- 5 - As reparações terão lugar no local de funcionamento do bem em causa.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 6 - A permanência do cocontratante nas instalações referidas no número anterior que implique paragem dos bens instalados deverá ocorrer fora das horas normais de serviço do local de funcionamento do bem em causa, salvo nas situações previamente autorizadas pela Entidade Adjudicante.
- 7 - Em casos em que manifestamente se verifique ser impossível a resolução do problema reportado no local dentro do prazo, deverá o cocontratante proceder à substituição temporária do equipamento enquanto decorrer a reparação em instalações próprias deste, mediante autorização escrita da Entidade Adjudicante.

Cláusula 23.ª
Entregáveis e documentação

- 1 - O cocontratante obriga-se a desenvolver os seguintes trabalhos:
 - a) Entrega de equipamentos, se aplicável;
 - b) Entrega de software e respetivo licenciamento;
 - c) Entrega dos serviços de implementação, nos termos da secção 9 do presente Caderno de Encargos;
 - d) Entrega da documentação prevista no Anexo A deste Caderno de Encargos.

Cláusula 24.ª
Formação

- 1 - O cocontratante obriga-se a ministrar a formação aos colaboradores da Entidade Adjudicante relativamente aos bens fornecidos, nos termos do Anexo A do presente Caderno de Encargos.
- 2 - A formação decorrerá nas instalações da Entidade Adjudicante ou, quando aceite por esta, também de forma remota, em prazo a acordar entre as partes, sem prejuízo do estabelecido no número um da Cláusula 19ª.
- 3 - O cocontratante não poderá exigir qualquer quantia adicional relacionada com a formação.

Cláusula 25.ª
Planeamento

- 1 - Deverá ser realizada uma atividade de planeamento, nos termos da secção 9.2 do Anexo A.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Cláusula 26.ª

Mecanismos formais de acompanhamento

- 1 - Serão realizadas reuniões quinzenais de ponto de situação do estado de execução do projeto, complementadas pela entrega dos relatórios de progresso correspondentes, podendo ser necessário ajustar essa periodicidade em função da evolução da dinâmica do projeto.
- 2 - Os relatórios de progresso referidos no número anterior, a disponibilizar em formato PDF, devem indicar o estado de execução dos trabalhos, um diagrama de Gantt atualizado com todas as tarefas e respetivas datas de execução, realizadas e pendentes, e ainda, a indicação das situações que requeiram a eventual intervenção da entidade adjudicante para manter a dinâmica do projeto dentro dos parâmetros de qualidade e calendário pretendidos.
- 3 - O estabelecido no número um não dispensa a realização das interações informais, entre os cocontratantes, com a dinâmica que se revele necessária para o bom andamento dos trabalhos.
- 4 - Durante a vigência do contrato, o adjudicatário deverá estar disponível para realizar as reuniões com o GRA, e entidades por si designadas, que se revelarem necessárias.
- 5 - A entidade adjudicante dispõe de um prazo de 15 dias, contados a partir da data de entrega de cada um dos relatórios R1, R2 e R3 (definidos na secção 9 do Anexo A), para proceder à respetiva análise e comunicar ao adjudicatário a sua aceitação ou solicitar quaisquer eventuais correções. O prazo referido será reduzido para 8 dias no caso de a análise incidir sobre uma versão que já tenha sido sujeita a correções na sequência de uma análise anterior.
- 6 - Durante o período a que respeita a tarefa descrita no número anterior, o prazo de execução do adjudicatário é suspenso.
- 7 - Na eventualidade da entidade adjudicante ter solicitado alterações, estas deverão ser realizadas pelo adjudicatário no prazo de 8 dias, sendo a nova versão do documento entregue novamente para avaliação.
- 8 - O processo descrito nos pontos 5 - a 7 - repetir-se-á até que o plano de execução seja integralmente aceite pela entidade adjudicante, sendo o cumprimento deste requisito determinante para que o adjudicatário possa iniciar os trabalhos de implementação.
- 9 - Decorrido o prazo aplicável e referido no ponto 7 - , sem que a entidade adjudicante se tenha pronunciado, considera-se tacitamente aceite a versão mais recente do plano de execução entregue pelo adjudicatário.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Cláusula 27.ª

Sanções

- 1 - Pelo incumprimento de obrigações emergentes do contrato, a Entidade Adjudicante pode exigir ao cocontratante o pagamento de uma sanção pecuniária, num montante a fixar em função da gravidade do incumprimento, nos termos definidos na secção 12 do Anexo A deste Caderno de Encargos.
- 2 - Na determinação da gravidade do incumprimento, a Entidade Adjudicante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do cocontratante e as consequências do incumprimento.
- 3 - A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida nota de crédito.
- 4 - O valor acumulado das sanções pecuniárias não pode exceder 20 % do preço contratual, sem prejuízo do poder de resolução do contrato.
- 5 - Nos casos em que seja atingido o limite previsto no número anterior e a Entidade Adjudicante decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30 %.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

ANEXO A – REQUISITOS FUNCIONAIS E TÉCNICOS

1 Enquadramento

- 1.1 A Cibersegurança posiciona-se atualmente como um fator determinante para a garantia do sucesso e da resiliência das sociedades, assim como das organizações e dos indivíduos que as integram. Com o desenvolvimento ubíquo das iniciativas e soluções que tornam a nossa vivência cada vez mais digital, importa estabelecer estratégias e mobilizar recursos capazes de dar resposta adequada às ameaças e aos riscos crescentes.
- 1.2 Neste contexto, o Governo Regional dos Açores (GRA) pretende criar um Centro de Operações de Cibersegurança (SOC), capaz de corresponder aos desafios conjunturais e às exigências colocadas pelos demais investimentos tecnológicos e de digitalização atuais e futuros.
- 1.3 No sentido de se dotar de ferramentas de cibersegurança e poder minimizar o impacto de potenciais ameaças, o GRA pretende implementar uma plataforma de monitorização e gestão de dispositivos para detetar e responder a incidentes de cibersegurança, cujo fornecimento, instalação e suporte constituem o objeto do presente procedimento.

2 Caracterização da situação atual

- 2.1 A entidade adjudicante dispõe de dois Centros de Dados gémeos, localizados nas ilhas de São Miguel e Terceira, que se encontram implementados numa configuração de alta disponibilidade e funcionalidades de *Disaster Recovery* que permitem assegurar a continuidade das operações centralizadas de IT do GRA em caso de falha de um deles.
- 2.2 Os dois Centros de Dados apresentam configurações e dimensionamento de hardware e software idênticos;
- 2.3 Estes Centros de Dados, implementados segundo uma configuração de alta disponibilidade (ativo-ativo) e com funcionalidades de *Disaster Recovery* bidirecional entre as duas instalações, suportam uma plataforma integrada de cloud privada e de virtualização de redes e sistemas baseadas na plataforma VMware (vSphere, vCenter e NSX-T).
- 2.4 Os sistemas de core switching de cada Centro de Dados assentam em dois equipamentos interligados numa configuração de alta disponibilidade.
- 2.5 Cada Centro de Dados possui um cluster de firewalls, numa configuração de alta disponibilidade, constituído por dois sistemas Palo Alto PA-5250.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 2.6 Atualmente encontra-se em produção uma solução de segurança de endpoints da Palo Alto (Cortex XDR), licenciada para 10.000 PCs/servidores.

3 Solução tecnológica pretendida

- 3.1 A solução pretendida deve disponibilizar as seguintes funcionalidades macro, conforme se detalha abaixo:
- a) Segurança dos endpoints;
 - b) SIEM (*Security information and event management*);
 - c) Análise de tráfego;
 - d) SOAR (*Security Orchestration Automation and Response*);
 - e) Gestão de vulnerabilidades.
- 3.2 As componentes de software a fornecer poderão ser instaladas na plataforma de virtualização referida no ponto 2.3, sem prejuízo da necessária satisfação dos requisitos de resiliência descritos no ponto 3.7, aplicáveis a qualquer arquitetura que venha a ser proposta.
- 3.3 Quaisquer soluções de hardware que, eventualmente, venham a ser propostas, devem respeitar igualmente os requisitos de resiliência descritos no ponto 3.7.
- 3.4 Todas as componentes tecnológicas a fornecer (hardware e software) devem ser do mesmo fabricante, de modo a garantir a total compatibilidade entre os vários sistemas.
- 3.5 A solução a propor deverá garantir a plena interoperabilidade com as firewalls referidas no ponto 2.5 e permitir a recolha automática de informação disponibilizada por estas.
- 3.6 A solução deve prever a renovação do licenciamento dos endpoints indicados no ponto 2.6 ou propor uma alternativa, desde que satisfaça os requisitos descritos na secção 4.
- 3.7 A solução deve apresentar uma configuração de alta disponibilidade, tanto ao nível das componentes de software quanto de hardware, caso existam, devendo assegurar o cumprimento dos seguintes requisitos de resiliência:
- a) Em cada Centro de Dados, a solução deverá poder recolher dados simultaneamente dos dois *switches* core instalados, a operarem numa configuração de alta disponibilidade, bem como de outros *switches* localizados remotamente;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- b) No caso de interrupção parcial ou total da operacionalidade da solução proposta num dos Centros de Dados (ou da paragem total ou perda de conectividade WAN/Internet do mesmo), as componentes instaladas no outro deverão continuar a recolher dados de todos os endpoints indicados no ponto 4.1.3 sem perda de funcionalidades;
 - c) A solução a fornecer não poderá apresentar pontos únicos de falha nem perder quaisquer funcionalidades ou registar interrupções de serviço, que resultem da paragem total de um dos Centros de Dados;
 - d) A solução não poderá perder quaisquer funcionalidades com a paragem total de um dos Centros de Dados.
- 3.8 O concorrente deverá propor todos os itens necessários para assegurar a total operacionalidade da solução especificada neste Caderno de Encargos, pela qual será responsável.
- 3.9 O concorrente deverá efetuar, na sua proposta, uma descrição tão detalhada quanto possível, em cada vertente técnica da solução, da seguinte informação, para além de outros aspetos que entenda relevantes para melhorar o entendimento da solução apresentada:
- a) Memória descritiva detalhada, caracterização do modelo conceptual, lógica/modo de funcionamento e arquitetura técnica;
 - b) Tecnologias, produtos e licenças de software;
 - c) Características funcionais e técnicas;
 - d) Dimensionamento das soluções propostas;
 - e) Requisitos em termos de capacidade de alojamento e/ou virtualização, a disponibilizar pela entidade adjudicante, quando a solução proposta seja baseada na utilização de máquinas virtuais e outras componentes de software;
 - f) Pressupostos assumidos pelo concorrente que influenciaram as características funcionais/técnicas, opções tomadas e dimensionamento propostos;
 - g) Listagens detalhadas dos itens que constituem a solução, indicando a função de cada um e as respetivas quantidades;
 - h) Diagramas de ligações lógicas e físicas, conforme for aplicável;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- i) Tipologias/débitos de interfaces de comunicação, conforme for aplicável;
 - j) Interdependências e fluxos de dados entre componentes/módulos/sistemas;
 - k) Datasheets de todos os componentes de hardware e/ou software, nos anexos da proposta.
- 3.10 O concorrente deverá entregar, juntamente com a sua proposta, uma declaração do fabricante fazendo prova de que este tem conhecimento do conteúdo da mesma e de que prestará todo o apoio necessário ao proponente na execução do projeto, na eventualidade do mesmo lhe ser adjudicado.

4 Segurança dos endpoints

4.1 Requisitos gerais

- 4.1.1 Pretende-se o upgrade do licenciamento associado à atual solução de segurança dos endpoints (referida no ponto 2.6), ou a proposta de uma solução substituta, com vista a garantir a prevenção, deteção e resposta a incidentes totalmente unificada e com uma interface de gestão única para os endpoints e para o tráfego de rede (on-prem ou cloud).
- 4.1.2 A solução proposta deve responder aos seguintes *use cases*:
- a) NTA (*Network Traffic Analytics*);
 - b) UEBA (*User Behaviour Analytics*);
 - c) EDR (*Endpoint Detection and Response*);
 - d) *Host Insights* com gestão de vulnerabilidades.
- 4.1.3 A instalação de, pelo menos, 10.000 postos de trabalho/servidores (endpoints).
- 4.1.4 Configuração de sensores com a capacidade de analisar pelo menos 65 TBs de tráfego de rede por mês.
- 4.1.5 A solução deve ser capaz de ingerir dados da rede do GRA (*on-premise* e *cloud*) de forma a ter visibilidade de todo o tráfego e efetuar deteção comportamental sobre a rede, endpoint e cloud numa única solução e interface gráfica.
- 4.1.6 Permitir a realização de análises forenses detalhadas dos ataques impedidos.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 4.1.7 Detetar anomalias no tráfego de rede e no comportamento dos utilizadores.
- 4.1.8 Módulo de Endpoint Detection and Response (EDR).
- 4.1.9 Módulo de visibilidade sobre as máquinas.
- 4.1.10 Prevenção contra exploits, incluindo aqueles que utilizam vulnerabilidades do tipo Zero-Day.
- 4.1.11 Prevenção contra a execução de malware, sem requerer qualquer conhecimento prévio.
- 4.1.12 Capacidade de restringir a execução de determinados ficheiros.
- 4.1.13 Proteger contra ransomware.
- 4.1.14 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.
- 4.1.15 Controlar dispositivos USB.
- 4.1.16 Disk Encryption.
- 4.1.17 Host Firewall.
- 4.1.18 Permitir isolar automaticamente da rede máquinas infetadas com malware.

4.2 Gestão

- 4.2.1 A solução proposta deve ser gerida através de uma interface gráfica web única.
- 4.2.2 A solução deve ter a capacidade de integrar com a plataforma de gestão das *firewalls* de rede existentes e correlacionar as duas componentes para obter análise forense tanto da componente de rede como dos processos dos endpoints.
- 4.2.3 A plataforma de gestão deve ter os seguintes menus principais: Reporting, Investigation, Response, Endpoints, Rules, Add-on e Assets.
- 4.2.4 A solução proposta deve poder exportar os seus logs em formato syslog para qualquer solução de gestão de logs.
- 4.2.5 A solução proposta deve ter uma gestão centralizada baseada em cloud.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 4.2.6 A solução deve vir de base já configurada com as best practices do fabricante de forma a simplificar o deployment da mesma.
- 4.2.7 A solução deve 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.
- 4.2.8 A solução proposta deve suportar a atualização de software dos agentes de endpoint diretamente a partir da cloud.

4.3 Prevenção de Exploits

- 4.3.1 A solução proposta deve permitir a proteção de processos do sistema operativo e aplicações, com a capacidade de adicionar à lista de aplicações protegidas, aplicações proprietárias de terceiras partes ou customizadas.
- 4.3.2 Deve oferecer proteção, em tempo real, contra exploits de qualquer vulnerabilidade aplicacional (incluindo do tipo zero-day ou desconhecidos) através do bloqueio de técnicas de exploits, tais como “Software Logic Flaws”, “Memory Corruptions”, “DLL Hijacking”, “heap spray”, “JIT”, “ROP” e “SEH”.
- 4.3.3 Deve garantir proteção contra 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.
- 4.3.4 Assim que a solução proposta detete ou bloqueie 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) e terminar apenas este processo.
- 4.3.5 Deve utilizar módulos de técnicas de exploit para prevenir ou bloquear exploits, não devendo basear a prevenção ou bloqueio de exploits em assinaturas, reputação e heurísticas dos ficheiros.
- 4.3.6 A solução proposta não pode 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, devendo ter um impacto mínimo no desempenho através da utilização de um agente leve e não intrusivo que pode ser totalmente invisível para o utilizador.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 4.3.7 Deve proteger de forma simultânea todas as aplicações e processos do endpoint contra técnicas de exploit.
- 4.3.8 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.
- 4.3.9 Deve conseguir proteger o endpoint contra “Kernel privilege escalation”.
- 4.3.10 A solução proposta deve também conseguir proteger contra exploits para MacOS e Linux como por exemplo “local privilege escalation”.

4.4 Prevenção de Malware

- 4.4.1 A solução proposta deve suportar proteção contra executáveis maliciosos.
- 4.4.2 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.
- 4.4.3 Deve ter a capacidade de controlar o que pode ser executado no endpoint, a partir de onde pode ser executado e com que parâmetros.
- 4.4.4 Deve impedir o lançamento de qualquer processo legítimo que possa ser utilizado para fins maliciosos, dado que esta técnica é muitas vezes utilizada em ataques de ransomware e outros malwares para fazer *bypass* à segurança do endpoint.
- 4.4.5 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).
- 4.4.6 Deve ser capaz de prevenir a execução de malware através da análise de comportamentos desencadeados pelo malware.
- 4.4.7 Deve garantir a possibilidade de configurar whitelists globais para permitir a execução de certos ficheiros executáveis.
- 4.4.8 Deve ser capaz de criar regras de exclusão das capacidades de proteção para endpoints específicos.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 4.4.9 Deve detetar e bloquear malware através do uso de machine learning e não deve utilizar assinaturas locais independentemente do sistema operativo.
- 4.4.10 Deve ser capaz de analisar ficheiros do tipo mach-o, ELF e APK.
- 4.4.11 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.
- 4.4.12 Deve conseguir perguntar aos serviços APT na cloud por valores de hash para verificar se determinado ficheiro é malicioso ou benigno.
- 4.4.13 Deve utilizar técnicas locais de machine learning para detetar malware desconhecido.
- 4.4.14 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.
- 4.4.15 Deve ter a capacidade de submeter aos serviços APT na cloud ficheiros potencialmente maliciosos.
- 4.4.16 Deve conseguir visualizar na plataforma de gestão centralizada os relatórios de análise do malware.
- 4.4.17 A solução proposta não deve analisar ficheiros que já tenham sido anteriormente submetidos aos serviços APT na cloud.
- 4.4.18 Deve conseguir bloquear malware desconhecido utilizando tecnologia APT sandbox na cloud e fornecer um relatório com o veredicto e análise do ficheiro submetido. A solução de APT sandbox na cloud deve ser do mesmo fabricante da solução proposta para garantir uma maior integração e compatibilidade.
- 4.4.19 Deve ter a capacidade de modificar manualmente a decisão tomada pelos serviços APT na cloud para uma hash em particular.
- 4.4.20 Deve ter a capacidade de bloquear a execução de um ficheiro no caso da sua hash ser desconhecida dos serviços APT na cloud.
- 4.4.21 Deve ter a capacidade de bloquear a execução de um ficheiro no caso do endpoint não conseguir contactar os serviços APT na cloud e o valor da hash do ficheiro não ser localmente conhecido.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 4.4.22 Deve garantir a capacidade de efetuar análises estáticas (machine learning) em modo offline para Windows, Linux e macOS.
- 4.4.23 Deve impedir processos que corram no endpoint de fazerem o carregamento de DLL's maliciosos. A solução proposta deve examinar os DLL's e criar um veredicto sobre se deve ou não ser executado o carregamento de determinado DLL.
- 4.4.24 Deve analisar comportamentos de ransomware antes da execução do mesmo e bloquear ataques baseados em encriptação através da análise em tempo real de atividades de encriptação.
- 4.4.25 Deve conseguir bloquear ataques que tirem partido do kernel para carregar e correr código "shell" malicioso.
- 4.4.26 O módulo de análise de comportamentos de ransomware deve poder operar em modo de notificação ou de bloqueio.
- 4.4.27 A solução proposta deve possuir um módulo de análise de comportamentos de ransomware que suporte os sistemas de ficheiros NTFS, FAT e exFAT.
- 4.4.28 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 fabricante específico ou com um número de série específico. Deverá ser possível criar políticas apenas temporárias.
- 4.4.29 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.
- 4.4.30 A solução deve suportar os seguintes sistemas operativos:
 - a) Android 5, 6, 7, 8, 9 e 10;
 - b) Debian 8 e 9;
 - c) CentOS 6 e 7;
 - d) Oracle 6 e 7;
 - e) Red Hat 6 e 7;
 - f) SUSE 12;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- g) Ubuntu 12, 14, 16 e 18;
- h) macOS 10.11, 10.12, 10.13, 10.14 e 10.15;
- i) Windows 7, 8, 10 e 11;
- j) Windows Server 2008R2, 2012, 2016 e 2019.

5 SIEM (*Security information and event management*)

- 5.1 A solução deve monitorizar todos os endpoints, nomeadamente informação relativa a processos, ficheiros, tráfego de rede, registry e memória. Qualquer atividade relacionada com estas tipologias de informação deve ser guardada no mínimo para os últimos 30 dias. Deverá ser possível prolongar esta retenção indefinidamente.
- 5.2 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.
- 5.3 A solução deve 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, sem ser necessário utilizar ou aprender uma nova query language.
- 5.4 Quando diferentes alertas estão relacionados, a solução deve ser capaz de os agregar automaticamente num único incidente.
- 5.5 Deve ser possível agregar diferentes incidentes num único.
- 5.6 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.
- 5.7 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.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 5.8 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 (p.e., VirusTotal).
- 5.9 A solução deve mapear os diferentes alertas para a Framework Mitre ATT&CK.
- 5.10 Para recolher o tráfego de rede, a solução deve ser capaz de integrar com pelo menos 4 fabricantes de Firewalls, incluindo os sistemas descritos na secção 2 deste anexo.
- 5.11 Deve ser possível ingerir logs de identity providers, nomeadamente: AzureAD, Okta e PingID de forma a detetar anomalias nos padrões de autenticação dos utilizadores.
- 5.12 Deve ser possível recolher e correlacionar logs de qualquer solução de segurança e rede existente via syslog e netflow. Deve também ser possível recolher informação diretamente de sistemas de base de dados.
- 5.13 A solução deve aprender o comportamento de cada máquina e criar perfis de forma a ser capaz de identificar comportamentos anómalos.
- 5.14 A solução deve ser capaz de aprender o comportamento de cada utilizador e criar “Score Cards” para cada utilizador com informação sobre as anomalias comportamentais dos mesmos.
- 5.15 A solução deve disponibilizar uma query language para criar relatórios e widgets customizáveis a partir da informação recolhida pelo agente.
- 5.16 Com base na aprendizagem comportamental para cada máquina e utilizador, a solução deverá gerar alarmística para os seguintes cenários:
- a) Sessão rara de SSH;
 - b) Uso de comandos fora do comum (arp -a, ipconfig, etc);
 - c) Processos raros a comunicar com máquinas fora da organização;
 - d) Processos a comunicar com máquinas externas que não são normalmente acedidas pelas máquinas da organização;
 - e) Scripts a comunicar com hosts externos;
 - f) Listagem de utilizadores do domínio;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- g) Comando de powershell anormal;
- h) Volume de conexões entre máquinas elevado.

5.17 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.

6 Análise de tráfego

6.1 Sondas de tráfego

6.1.1 Com vista a reforçar a segurança dos segmentos de rede que não estão a ser cobertos pelas suas soluções de segurança de perímetro, pretende-se implementar sondas em pontos estratégicos da rede com os seguintes objetivos:

- a) Monitorizar o tráfego existente na organização;
- b) Identificar que utilizadores acedem aos diferentes serviços e aplicações do Data Center;
- c) Inspeccionar tráfego cifrado;
- d) Obter visibilidade sobre todo o tipo de aplicações em uso e respetivo nível de risco;
- e) Detetar tentativas de ataque e intrusão dentro da rede da organização.

6.1.2 Deverão ser fornecidas e instaladas, pelo menos, quatro sondas (i.e., duas por Centro de Dados) com as seguintes características de performance e capacidade:

- a) Performance da sonda com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção) $\geq$ 16 Gbps;
- b) Performance da sonda com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) $\geq$ 8 Gbps;
- c) Performance da sonda com a funcionalidade de VPN IPSec $\geq$ 6 Gbps;
- d) Número de novas sessões por segundo $\geq$ 120.000;
- e) Número máximo de sessões $\geq$ 10.000.000;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- f) Número de CPUs suportados ≤ 16 ;
 - g) Capacidade de memória RAM dedicada ≥ 56 GB;
 - h) Capacidade de unidade de disco dedicado ≥ 60 GB.
- 6.1.3 No caso das sondas serem baseadas numa solução de software, deverão poder ser instaladas em máquinas virtuais em VMware ESXi™, KVM e Microsoft Hyper-V, ou em clouds privadas incluindo VMware NSX-T, Cisco ACI, OpenStack e Nutanix AOS.
- 6.1.4 A solução deve poder utilizar como sensores na rede, as firewalls de pelo menos 4 fabricantes distintos, incluindo os sistemas referidos no ponto 2.5.
- 6.1.5 Deve ser possível colocar sensores em ambientes de cloud, nomeadamente, Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).
- 6.1.6 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.
- 6.1.7 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.
- 6.1.8 A solução deverá ser capaz de detetar o seguinte tipo de eventos:
- a) Malware a ser transmitido na rede;
 - b) Máquina a enviar SPAM;
 - c) Máquina com um número anormal de conexões falhadas para outros endpoints;
 - d) Elevado número de conexões para um determinado porto que não corresponde ao perfil;
 - e) Port Scan;
 - f) Conexões consecutivas entre 2 endpoints que não são normais;
 - g) Novos comportamentos do administrador;
 - h) Execução remota de comandos;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- i) Reverse Shell;
- j) Tráfego SMB/KRB através de um protocolo inesperado;
- k) DNS Tunneling;
- l) Número anormal de resoluções de DNS falhados;
- m) DGA (Domain Generated Algorithm);
- n) Command and Control através da análise de pedidos de DNS, URLs e ligações diretas a IPs;
- o) Tunneling;
- p) Volume anormal de dados transferidos.

6.1.9 No caso de ser identificado um comportamento malicioso na rede, deve ser possível obter informação sobre os processos da máquina afetada mesmo que esta não tenha nenhum agente instalado.

6.2 Visibilidade sobre as máquinas

6.2.1 A solução deve incluir um módulo de visibilidade com as características seguidamente descritas.

6.2.2 Capacidade de identificar os seguintes objetos:

- a) Utilizadores e grupos configurados em cada máquina;
- b) Serviços a correr nas máquinas;
- c) Drivers instalados nas máquinas;
- d) Processos, drivers e serviços que são automaticamente inicializados sempre que o utilizador inicia a sua máquina;
- e) Shares de rede configuradas nas máquinas;
- f) Discos existentes nas máquinas.

6.2.3 Funcionalidade de “search & destroy” que permite pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

6.2.4 Identificar vulnerabilidades e respetiva criticidade para ambientes Windows e Linux.

6.2.5 Identificar as aplicações a correr em cada equipamento.

6.3 Resposta a incidentes

6.3.1 A solução proposta deve permitir iniciar scans de malware à máquina infetada.

6.3.2 Deve ser possível efetuar blacklists e whitelists a hashes.

6.3.3 Deve ser possível fazer quarentena a determinados processos.

6.3.4 Durante a investigação de um incidente, a solução deve permitir isolar da rede máquinas infetadas.

6.3.5 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.

6.3.6 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.

6.3.7 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.

6.3.8 Capacidade de criar regras de correlação personalizadas que permitem detetar ataques retroativamente.

6.3.9 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.

7 SOAR (*Security Orchestration Automation and Response*)

7.1 Requisitos gerais

7.1.1 Pretende-se adotar uma solução de SOAR (*Security Orchestration Automation and Response*), que permita orquestrar e automatizar o processo de resposta a incidentes da organização.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 7.1.2 Com esta solução deverá ser possível integrar as diferentes ferramentas utilizadas pelo SOC, automatizar e documentar o processo de investigação de incidentes, eliminar tarefas manuais repetitivas e gerir centralmente todos os incidentes da organização.
- 7.1.3 A solução deve utilizar playbooks de forma a automatizar os passos seguidos pelos analistas para responder aos diferentes tipos de incidentes (phishing, malware, etc.) desde o processo de triagem até ao fecho do incidente.
- 7.1.4 Permitir colaboração em tempo real entre os analistas de forma a acelerar o processo de resolução de um incidente.
- 7.1.5 Permitir centralizar toda a componente de *ticketing* e gestão de incidentes para a equipa do SOC.
- 7.1.6 A solução deve disponibilizar um módulo de *Threat Intelligence Management* que permita automatizar o processo de ingestão, classificação e utilização de *feeds*.
- 7.1.7 A componente de automação da plataforma deve basear-se no uso de *workflows* modulares e scripts. Qualquer tarefa que seja automatizada deve poder ser visualizada através de um *workflow* disponível na interface gráfica.
- 7.1.8 Deve ser disponibilizada uma aplicação móvel onde um analista ou *SOC manager* possa obter informação sobre incidentes ativos, SLAs e *system health* entre outros. Esta aplicação deve ser suportada em iOS e Android.
- 7.1.9 A solução deverá permitir o acesso simultâneo de, pelo menos, quatro analistas de segurança e um auditor.

7.2 Arquitetura

- 7.2.1 A arquitetura da solução deve permitir realizar deployments on-premises e cloud.
- 7.2.2 No caso de deployments cloud não deve ser necessário que as ferramentas internas comuniquem diretamente com a cloud. A arquitetura da solução deve garantir que qualquer ferramenta que necessite de comunicar com a cloud, o possa fazer através de um proxy disponibilizado pela solução.

7.3 Playbooks

- 7.3.1 A solução deve suportar a utilização de playbooks, de modo a que determinadas medidas sejam executadas automaticamente, quando ocorra um incidente.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 7.3.2 Por defeito, a plataforma deve ter mais de 100 playbooks configurados que correspondam a diferentes use cases e tipos de incidentes.
- 7.3.3 Os playbooks devem ser opensource. Qualquer pessoa com uma conta do GitHub deve poder submeter updates.
- 7.3.4 Deve ser possível criar playbooks novos de raiz ou a partir da cópia e edição de playbooks existentes. Estes playbooks devem ser criados usando um editor que permita configurá-los através de uma interface gráfica que utilize mecanismos de drag-and-drop. Não deve ser necessário desenvolver código para a criação de playbooks. As tasks executadas por estes playbooks podem ser baseadas em tasks já existentes ou criadas de raiz.
- 7.3.5 Deve ser possível incluir playbooks dentro de outros playbooks.
- 7.3.6 Os playbooks podem conter tasks manuais, tasks automatizadas, filtros, sub playbooks, tasks de recolha de dados e tasks condicionais.
- 7.3.7 Deve ser possível correr playbooks automaticamente assim que um incidente é gerado na plataforma. Também deve ser possível agendar playbooks para correr em determinados períodos de tempo.
- 7.3.8 Deve ser possível correr playbooks manualmente através da criação de um incidente no sistema e da sua associação com um playbook. Os Playbooks também devem poder ser criados como “Jobs” e ser corridos em tempo real para determinados use cases (p.e., health check).
- 7.3.9 A representação gráfica de cada componente dos playbooks deve servir como um nível de abstração para os scripts e funções automatizadas que correm no backend.
- 7.3.10 Todos os outputs de um playbook devem ser documentados no sistema, assim como as atividades do analista.
- 7.3.11 Deve ser possível criar tasks no processo de investigação que necessitem de interação com o analista para progredir na análise do incidente.
- 7.3.12 A execução dos playbooks deve poder ser visualizada passo a passo em tempo real, ou à posteriori, através de uma ferramenta de *debugging*.
- 7.3.13 No caso de algum dos passos do playbook parar devido a um erro, deve ser possível recomençar o playbook a partir deste passo.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 7.3.14 Deve ser possível mapear nos playbooks os processos e procedimentos CIRT atuais e futuros para “Incident Types”.
- 7.3.15 Deve ser possível atribuir tarefas dentro de um playbook a diferentes membros da equipa.
- 7.3.16 O output de qualquer task dentro de um playbook deve poder ser consumido por qualquer outra task que seja executada posteriormente nesse workflow.
- 7.3.17 Tasks que façam parte do workflow de um playbook devem poder consumir outputs gerados por sub-playbooks que tenham sido executados previamente nesse workflow.
- 7.3.18 Deve ser mantido o histórico de todos os playbooks e tasks executados no sistema.
- 7.3.19 Deve ser possível exportar playbooks.
- 7.3.20 Todos os playbooks devem manter um sistema de “versioning”.
- 7.3.21 Devem existir playbooks específicos para lidar com incidentes de ransomware.
- 7.3.22 Devem existir playbooks específicos para lidar com incidentes relacionados com GDPR.
- 7.3.23 A plataforma deve disponibilizar out of the box playbooks para use cases fora do mundo tradicional da segurança, nomeadamente, *onboarding* de novos empregados, *offboarding* de empregados, ativação de utilizadores na AD, atribuição de acessos a novos utilizadores, e Shadow IT, entre outros.

7.4 REST API

- 7.4.1 A solução deve ter uma API que permita executar as mesmas operações que estão disponíveis via interface gráfica.

7.5 Gestão de Incidentes

- 7.5.1 A solução deve integrar com ferramentas de *ticketing*, nomeadamente Jira, RSA Archer, ServiceNow, Micro Focus Service Manager, Remedy, Easyvista, Salesforce, Zendesk e Freshdesk. As integrações devem ser bidirecionais de forma a iniciar ações para a criação de tickets assim como pesquisar e atualizar tickets existentes.
- 7.5.2 A solução deve ter o seu próprio sistema de *ticketing* que deve poder ser utilizado pela equipa de segurança/SOC.
- 7.5.3 Deve ser possível atribuir incidentes a utilizadores e a equipas.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 7.5.4 Deve ser possível especificar SLAs para os diferentes tipos de incidentes.
- 7.5.5 A plataforma deve permitir gerir e monitorizar SLAs.
- 7.5.6 Deve ser possível enviar notificações para a equipa interna assim como para os utilizadores finais. Integrações com ferramentas como Okta, Slack ou email para este efeito também devem estar disponíveis. Estas notificações devem poder ser geradas quando existem alterações num incidente, como parte de um playbook, para avisos relativos a SLAs, ou outros parâmetros.
- 7.5.7 Deve ser utilizada uma REST API para obter informação de outras plataformas de forma a gerar incidentes.
- 7.5.8 Deve ser possível agrupar incidentes relacionados.
- 7.5.9 A plataforma deve utilizar Machine Learning para detetar incidentes duplicados.
- 7.5.10 Deve ser possível customizar incidentes, nomeadamente permitir aos utilizadores da plataforma criar tipos de incidentes customizáveis, campos/labels customizáveis, tipos de indicadores customizáveis, layouts para o sumário dos incidentes customizáveis, dashboards customizáveis e relatórios customizáveis.
- 7.5.11 A solução deve permitir o mapeamento automático dos campos de cada caso assim que o incidente é criado.
- 7.5.12 Deve ser possível utilizar tags na criação de tickets.
- 7.5.13 A solução deve permitir delegar tarefas a outros utilizadores.
- 7.5.14 A solução deve ser capaz de detetar alertas redundantes e agregá-los num único ticket.
- 7.5.15 A solução deve automaticamente processar os incidentes antes de o analista começar qualquer investigação.

7.6 Documentação

- 7.6.1 A plataforma deve permitir documentar todas as ações tomadas na análise de qualquer tipo de incidente.
- 7.6.2 Todos os incidentes devem disponibilizar uma secção na interface gráfica que documente todas as alterações efetuadas, membros da equipa envolvidos no incidente, tasks completas, IOCs, comandos executados manualmente pelos analistas, evidências, chat,



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

notas, tasks do playbook e seu respectivo output. Esta informação deve ser apresentada de forma a respeitar a timeline dos acontecimentos.

- 7.6.3 Qualquer output gerado pelos playbook ou comandos executados manualmente pelos analistas deve poder ser marcado como evidência de forma a justificar a decisão final em relação ao incidente. Este processo deve poder ser automatizado através da sua integração com as tasks do playbook.
- 7.6.4 A “Chain of custody” deve estar documentada.
- 7.6.5 Devem existir timestamps para cada incidente.
- 7.6.6 As ações dos analistas devem ser documentadas.
- 7.6.7 Deve ser possível utilizar campos customizáveis para mapear IOCs para as respetivas fases da “Kill Chain”.

7.7 Colaboração

- 7.7.1 A plataforma deve disponibilizar a sua própria ferramenta de colaboração para analistas. Cada incidente deve disponibilizar um “war room” onde os analistas podem colaborar entre si e partilhar informação sobre a investigação em curso.
- 7.7.2 O War Room deve permitir aos analistas colaborar, documentar e executar comandos de segurança numa única consola.
- 7.7.3 A solução deve também integrar com plataformas externas de colaboração como Microsoft Teams, Slack, Hipchat ou Mattermost.
- 7.7.4 No caso de os analistas utilizarem uma plataforma de colaboração durante a análise de incidentes, deve ser possível integrar o conteúdo desse chat com a plataforma e o respetivo incidente.
- 7.7.5 Deve ser possível convidar utilizadores externos à equipa de segurança de forma a estes terem acesso à plataforma de colaboração para determinados incidentes. A interação com utilizadores externos pode ser também feita através do envio de emails que pode ser despoletado através de uma task de um playbook. Estes playbooks devem monitorizar as respostas a estes emails e tomar ações dependendo da resposta obtida.
- 7.7.6 O produto deve permitir a transferência de conhecimento entre analistas.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

7.8 Repositório de indicadores

- 7.8.1 A solução deve possuir um repositório de indicadores.
- 7.8.2 A solução deve incluir playbooks automatizados de threat hunting.
- 7.8.3 Deve ser possível importar ficheiros STIX.
- 7.8.4 A estrutura dos indicadores deve poder ser customizada.
- 7.8.5 Deve ser possível correlacionar indicadores e incidentes.
- 7.8.6 A solução deve permitir gerir whitelists de indicadores.
- 7.8.7 Deve existir a capacidade de exportar indicadores para um ficheiro STIX.

7.9 Integração com ferramentas externas

- 7.9.1 A solução deve disponibilizar um Marketplace com o objetivo de instalar, trocar, contribuir e gerir todo o conteúdo da plataforma incluindo *playbooks*, automações, integrações, campos e *layouts*, entre outros.
- 7.9.2 O Marketplace deve permitir o acesso a conteúdos (p.e., integrações e playbooks) partilhados por outras organizações.
- 7.9.3 A solução deve integrar com, pelo menos, 20 ferramentas de análise forense, incluindo, Any.Run, CheckPoint Sandblast Appliance, CheckPoint Sandblast Cloud Services, malwr, McAfee Advanced Threat Defence, Palo Alto Networks WildFire, Rekall e VMRay.
- 7.9.4 A solução deve integrar com, pelo menos, 20 ferramentas de colaboração, incluindo, ActiveMQ, Cisco Webex Teams, Microsoft Teams, EWS, FCM Push Notifications e Kafka.
- 7.9.5 A solução deve suportar, pelo menos, 30 ferramentas de SIEM e análise de logs, incluindo, ArcSight, RSA Netwitness, IBM Qradar, Securonix, Exabeam, LogRhythm, Splunk, JASK, ELK, McAfee ESM e AlienVault.
- 7.9.6 A solução deve suportar, pelo menos, as seguintes ferramentas de endpoint: McAfee, Symantec, Trend, FireEye, CrowdStrike, Cylance, Sentinel One, Cisco AMP, CybeReason, ATP e Cortex XDR.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 7.9.7 A solução deve suportar, pelo menos, as seguintes plataformas de segurança de rede: Check Point, Palo Alto Networks, Forcepoint, Cisco, FireEye, Awake Security, Fortinet e Symantec.
- 7.9.8 A solução deverá suportar mais de 70 ferramentas de threat intelligence, como por exemplo, AlienVault, AWS Sagemaker, Anomali e urlscan.io.
- 7.9.9 A solução deve permitir a integração com pelo menos 650 ferramentas/serviços de IT e segurança.
- 7.9.10 Para além das integrações out of the box, a plataforma deve ter a funcionalidade de BYOI (Bring Your Own Integration).
- 7.9.11 A solução deve permitir desenvolver novas integrações de forma a garantir a interoperabilidade com ferramentas desenvolvidas in-house. De forma a poder criar estas integrações, a plataforma deve disponibilizar um SDK que permita criar novas integrações utilizando as linguagens Python ou Javascript.
- 7.9.12 Deve ser possível modificar o código de qualquer integração suportada na plataforma e utilizar este código para criar novas integrações.
- 7.9.13 A solução deve poder conectar-se a múltiplas instâncias de qualquer ferramenta com a qual integre.
- 7.9.14 Deve ser possível fazer upload para a plataforma de integrações customizadas de modo a integrar com produtos que não sejam suportados nativamente.
- 7.10 Reporting**
 - 7.10.1 A solução deve conter reports pré-definidos.
 - 7.10.2 Para cada incidente deve ser gerado um relatório automaticamente com o respetivo sumário.
 - 7.10.3 A solução deve permitir a criação de relatórios utilizando, pelo menos, 300 *widgets* predefinidos, assim como *widgets* customizáveis.
 - 7.10.4 Deve ser possível extrair relatórios usando os formatos PDF, DOC, CSV e HTML.
 - 7.10.5 Cada analista deve poder criar os seus próprios dashboards e relatórios. Devem também ser possível partilhá-los entre utilizadores da solução.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

7.11 Machine Learning

- 7.11.1 A solução deve ser capaz de sugerir quais os analistas que devem trabalhar em determinados incidentes tendo em conta o comportamento habitual da equipa e as áreas de foco de cada técnico.
- 7.11.2 A solução deve ser capaz de aprender e sugerir que ações devem ser tomadas pelo analista tendo em conta a análise de incidentes prévios.
- 7.11.3 A solução deve utilizar machine learning para identificar incidentes relacionados e incidentes duplicados.
- 7.11.4 A solução deve ser capaz de identificar e classificar emails de phishing através de machine learning.

7.12 Updates

- 7.12.1 Deve ser possível atualizar as integrações, os playbooks, os scripts de automação e os relatórios em ambientes offline.
- 7.12.2 Deve ser possível atualizar as integrações, os playbooks, os scripts de automação e os relatórios sem ter de fazer upgrade ao sistema.

7.13 Threat Intel Management (TIM)

- 7.13.1 A plataforma deve possuir um módulo de TIP (*Threat Intelligence Platform*) de modo a combinar as capacidades de SOAR e TIP numa única plataforma.
- 7.13.2 Deve ser possível consumir “*threat feeds*” de soluções comerciais, opensource e soluções criadas e partilhadas pela comunidade de cibersegurança.
- 7.13.3 A solução deve incluir feeds de threat intelligence do próprio fabricante.
- 7.13.4 A solução deve suportar formatos de dados não estruturados como email, news e RSS feeds.
- 7.13.5 Este módulo deve permitir criar incidentes na plataforma.
- 7.13.6 A solução deve suportar formatos de dados estruturados, nomeadamente, OpenIOC, Yara, STIX 1.0, STIX 1.2, STIX 2.0, XML, CSV e JSON.
- 7.13.7 A solução deve permitir classificar os feeds recebidos.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 7.13.8 Deve ser possível utilizar playbooks para processar os feeds, classificá-los e automatizar tarefas de threat hunting.
- 7.13.9 A solução deve permitir, através de playbooks, executar ações tais como adicionar IPs e domínios à blacklist de uma firewall (incluindo as referidas no ponto 2.5) ou bloquear uma hash numa solução de endpoint.
- 7.13.10 Deve ser possível correr playbooks para enriquecer os indicadores obtidos através de diferentes feeds.
- 7.13.11 Deve ser possível estabelecer relações entre indicadores de forma a facilitar o processo de análise dos mesmos.
- 7.13.12 A solução deve integrar com a *framework* MITRE ATT&CK e deve ser capaz de ingerir todas as técnicas e táticas que lhe estejam associadas. Deve ser possível associar estas técnicas e táticas a incidentes e executar determinados playbooks consoante as técnicas e táticas identificadas.
- 7.13.13 A solução deve conter playbooks baseados em “Courses of Action” que definam e automatizem todos os passos que devem ser tomados pela equipa de Incident Response quando um incidente classificado com uma determinada técnica e tática do MITRE é identificado.

8 Gestão de vulnerabilidades

- 8.1 No sentido de tornar a rede do GRA Zero Trust Complaint, pretende-se ter visibilidade total ao nível de quaisquer dispositivos na rede e dos riscos e vulnerabilidades associadas, e criar padrões de comportamento desses dispositivos de forma que a própria ferramenta sugira, automaticamente, políticas de segurança, para evitar ameaças e manter os dispositivos seguros.
- 8.2 A solução fornecida deve disponibilizar um repositório de dados de segurança (Data Lake), na cloud, de modo a suportar use cases, incluindo NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB (Cloud Access Security Broker), que envolvam a correlação transversal de informação entre todas as componentes e/ou produtos que integram a solução especificada neste Caderno de Encargos.
- 8.3 A solução deve colecionar metadados do tráfego de rede dos dispositivos, gerar logs com estas informações e enviá-los para um repositório de dados. Deve existir a capacidade de



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

analisar estes metadados através de um motor baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos na rede.

- 8.4 A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses.
- 8.5 O motor de identificação deve possuir três níveis:
- a) Identificação da categoria do dispositivo (p.e., câmara de videovigilância);
 - b) Identificação do seu perfil (p.e., fabricante, modelo e versão);
 - c) Identificação de cada instância do dispositivo.
- 8.6 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.
- 8.7 Quando é observado um comportamento anormal, a solução deve desencadear automaticamente regras de segurança, a aplicar nas firewalls existentes, que bloqueiem qualquer ligação anormal sem, todavia, prejudicarem o correto funcionamento do dispositivo.
- 8.8 A solução deve permitir a criação de regras nas firewalls existentes, baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão, sem ser necessário criar regras com base em IPs ou zonas.
- 8.9 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, entre outros.
- 8.10 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 (p.e., Uso de credenciais atribuídas por defeito).



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

9 Serviços de implementação

9.1 Requisitos gerais

- 9.1.1 O fornecimento dos bens objeto do presente Caderno de Encargos deverá ser suportado da prestação dos seguintes serviços de implementação, nos termos abaixo descritos:
- a) Serviço S1 – Planeamento da implementação;
 - b) Serviço S2 – Instalação, configuração, teste e otimização da solução;
 - c) Serviço S3 – Formação.
- 9.1.2 Os recursos do adjudicatário, a envolver no projeto, devem possuir as certificações técnicas do fabricante, adequadas às funções a desempenhar por cada um, que deverão ser entregues à entidade adjudicante, aquando da comunicação formal da adjudicação.
- 9.1.3 A entidade adjudicante reserva-se o direito de recusar a intervenção de recursos que não possuam as certificações referidas no ponto anterior.
- 9.1.4 O adjudicatário deverá nomear um gestor de projeto, com habilitações e experiência alinhadas com o perfil deste projeto, que assegure a coordenação de todos os recursos mobilizados e atividades desenvolvidas pelo adjudicatário, bem como a devida articulação dos trabalhos com a entidade adjudicante.

9.2 Serviço S1 – Planeamento da implementação

- 9.2.1 Antes de ser iniciada a instalação da solução especificada neste Caderno de Encargos, o adjudicatário deverá realizar um levantamento e planeamento pormenorizados cujos resultados deverão ser consubstanciados num plano de execução, elaborado nos termos do ponto 9.2.3 e que abranja todas as vertentes do projeto.
- 9.2.2 O processo de planeamento, referido no número anterior, deverá ser realizado através de várias sessões de trabalho, com a participação dos técnicos da entidade adjudicante, com vista a garantir a harmonização da solução a implementar com as infraestruturas e sistemas existentes, assegurar o alinhamento detalhado de expectativas e pressupostos entre as partes e, ainda, evitar disrupções operacionais não programadas durante os trabalhos de instalação, configuração, teste e otimização da solução adjudicada.
- 9.2.3 O plano de execução, designado por “Relatório R1 – Plano de Execução” deverá conter a descrição detalhada dos resultados deste serviço, todos os aspetos e pormenores técnicos



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

que caracterizam a solução objeto do presente Caderno de Encargos, incluindo os desenhos técnicos aplicáveis, mapas de quantidades, todas as atividades e tarefas a desenvolver com indicação das respetivas interdependências e calendário detalhado de execução na forma de um diagrama de *Gantt* representado com a granularidade temporal de uma semana.

- 9.2.4 O plano de execução deverá ser elaborado e entregue pelo adjudicatário no prazo máximo de 30 dias, a contar da data de início da vigência do contrato.

9.3 Serviço S2 – Instalação, configuração, teste e otimização da solução

- 9.3.1 Após a conclusão do Serviço S1 – Planeamento da implementação, nos termos do ponto 9.2, o adjudicatário procederá à instalação, configuração, teste e otimização da solução.

- 9.3.2 A prestação deste serviço deverá, no mínimo, prever a realização das seguintes tarefas, para além de outras que o concorrente eventualmente entenda serem relevantes para a qualidade do projeto, as quais deverá descrever na sua proposta:

- a) Instalação das componentes de software e de hardware (caso esteja previsto o seu fornecimento) nos dois Centros de Dados da entidade adjudicante;
- b) Instalação de 10.000 de agentes (endpoints) nos postos de trabalho e servidores definidos pelo GRA. A instalação dos agentes será realizada de forma remota, pelo adjudicatário, mas a partir das instalações da entidade adjudicante;
- c) Configuração da solução, nos termos estabelecidos no plano de execução;
- d) Testes de operacionalidade da solução implementada, nos termos dos pontos 9.3.4 e 9.3.5;
- e) Recolher, armazenar, correlacionar e analisar os registos reportados e emitir alertas de acordo com os casos de utilização identificados;
- f) Configurar um módulo de análise comportamental para definir alertas baseados em comportamentos que não cumpram a política de segurança;
- g) Avaliação da segurança global da rede do GRA (recorrendo à solução instalada) com deteção de potenciais vulnerabilidades e elaboração de um plano de remediação. O plano de remediação deverá efetuar uma distinção clara entre as ações corretivas desencadeadas automaticamente pela solução implementada, as otimizações a realizar à configuração da própria solução implementada (da responsabilidade do



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

adjudicatário) e as ações de reforço da segurança que se encontrem no âmbito da responsabilidade da entidade adjudicante;

h) Criar quatro *playbooks* na solução de SOAR que devem ter o seguinte âmbito:

- i. *Phishing*;
 - ii. Integração com a Active Directory do GRA;
 - iii. Integração com o Office 365 do GRA;
 - iv. Integração com IOC's de *feeds* do Centro Nacional de Cibersegurança.
- i) Implementar indicadores de compromisso e integrar nas plataformas existentes para melhorar as regras de segurança (sondas de rede, alterações de configuração inexplicáveis, comportamento incomum nas contas dos utilizadores, etc.), e integrações com a solução de Endpoint protection;
- j) Efetuar análises "post-mortem" a incidentes de segurança e atividades forenses, se necessário (exemplo: histórico de utilizadores, análise de registos web, entre outros);
- k) Realizar investigações básicas e mais avançadas, de nível forense, caso seja necessário (exemplo: análise da origem do incidente de segurança);
- l) Integração da Ferramenta de SOAR com o serviço de Ticketing do GRA em produção.

9.3.3 Os resultados da prestação deste serviço deverão ser integrados num relatório, designado por "Relatório R2 – Relatório de Implementação", que deverá incluir a seguinte informação, relativamente à solução instalada, para além de outros dados que o concorrente eventualmente entenda serem relevantes:

- a) Memória descritiva detalhada da solução técnica e da sua lógica de funcionamento, para cada uma das vertentes de implementação abrangidas;
- b) Representação gráfica detalhada da arquitetura de sistemas da solução implementada, tanto em termos físicos e/ou lógicos, consoante for aplicável;
- c) Diagramas detalhados, e devidamente legendados, de rede física e lógica para interligação dos diversos equipamentos e sistemas, quando aplicável;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- d) Mapas e diagramas representativos da estrutura de endereçamento IP estabelecida e subnets criadas, considerando as particularidades operacionais específicas de cada Centro de Dados, da segurança e de Disaster Recovery;
- e) Descrição detalhada das parametrizações efetuadas em todas as vertentes da solução (hardware, firmware e software), de modo a poderem ser replicadas manualmente, caso tal se revele necessário, devendo ser acompanhadas dos respetivos *print screens*;
- f) Complementarmente ao solicitado na alínea anterior, deverá ser apresentada uma descrição detalhada das atividades desenvolvidas e dos resultados obtidos, relativamente aos trabalhos especificados no ponto 9.3.2 do presente Caderno de Encargos;
- g) Deverão ser descritos de forma fundamentada, quais as decisões e pressupostos técnicos adotados, e acordados com a entidade adjudicante, para a instalação e customização da solução, nas suas diferentes vertentes, quando se trate de informação complementar à apresentada no Relatório R1 do plano de execução;
- h) Quadro de inventariação de todo o hardware, software e licenciamento instalado, devendo conter, no mínimo, a seguinte informação, conforme for aplicável ao tipo de solução proposta:
 - i. N.º ordem sequencial que identifique univocamente o bem fornecido neste quadro;
 - ii. Referência do fabricante;
 - iii. Designação atribuída;
 - iv. Função base que desempenha;
 - v. Marca e modelo, quando haja lugar ao fornecimento de hardware;
 - vi. Número de série, quando haja lugar ao fornecimento de hardware;
 - vii. Características técnicas;
 - viii. Atributos de dimensionamento e capacidade;
 - ix. Componentes de software instaladas e respetivas versões, quando aplicável;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- x. Designação do Centro de Dados em que se encontra instalado;
- xi. Referência do bastidor em que se encontra instalado, quando aplicável;
- xii. Fotografia do equipamento, instalado e ligado no respetivo bastidor, quando haja lugar ao fornecimento de hardware.
- xiii. Quadro de inventariação de todas as ligações físicas efetuadas;
- xiv. Manual com descrição dos procedimentos técnicos de *Disaster Recovery* da solução fornecida, a executar pela equipa do GRA (recuperação do incidente e posterior reposição da normalidade), nos casos em que a solução de segurança fornecida seja passível de sofrer impactos operacionais, quando o GRA tenha de ativar os procedimentos de recuperação de desastre ou de reposição do funcionamento num dos Centros de Dados.

9.3.4 Após a conclusão da instalação e configuração da solução proposta, o adjudicatário deverá realizar um conjunto de testes de operacionalidade que permitam validar o correto funcionamento da solução, de acordo com as especificações do presente Caderno de Encargos, bem como a sua capacidade para manter a continuidade de funcionamento dos serviços disponibilizados por esta, em caso de deficiência no funcionamento de quaisquer dos seus componentes, com vista a identificar oportunidades de melhoria que possam ser incorporadas antes da conclusão do processo de implementação.

9.3.5 Os testes referidos no ponto anterior deverão englobar as seguintes vertentes:

- a) Testes de conformidade para avaliar o cumprimento dos requisitos funcionais e técnicos da solução, em condições normais de funcionamento, estabelecidos neste Caderno de Encargos;
- b) Testes de tolerância a falhas para avaliar a resiliência da solução, em caso de ocorrência de falhas isoladas nalguma das suas componentes, verificando se são cumpridos os pressupostos de alta disponibilidade, estabelecidos neste Caderno de Encargos, bem como na informação complementar apresentada na proposta do adjudicatário;
- c) Testes de recuperação de desastre e reposição para avaliar a eficácia da solução quando exista a necessidade de transferir a operacionalidade de todos os serviços residentes no Centro de Dados em falha total, para o outro, bem como a reposição da normalidade, com o maior grau de automatização possível;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- d) Testes de desempenho para validar o cumprimento dos níveis mínimos especificados no ponto **Erro! A origem da referência não foi encontrada.**;
- e) Testes de segurança e de intrusão de rede aos sistemas fornecidos no âmbito deste procedimento, seguidas da aplicação das respetivas medidas corretivas, quando necessário;
- f) Outros testes que o adjudicatário entenda serem necessários à correta verificação da plena operacionalidade e segurança da solução.

9.4 Serviço S3 – Formação

9.4.1 O adjudicatário deverá executar um programa de transferência de conhecimento, de perfil simultaneamente teórico e prático, que permita aos técnicos do SOC do GRA adquirirem os conhecimentos necessários para:

- a) Exercerem um domínio eficaz nas atividades de operação, administração e manutenção da solução fornecida, em todas as suas vertentes;
- b) Assimilarem os detalhes da forma como a solução foi implementada e dos critérios utilizados;
- c) Atuarem com eficácia na resposta a incidentes e em atividades de análise forense.

9.4.2 O programa será dirigido a uma equipa de 10 técnicos, nomeados pela entidade adjudicante e realizado em instalações da entidade adjudicante.

9.4.3 Deverão ser entregues, aos participantes neste programa, os seguintes materiais de suporte:

- a) Manuais de e/ou cópias dos slides apresentados, em formato digital e em papel, relativamente a cada módulo ministrado;
- b) Certificados de participação;
- c) Acesso gratuito a exame de certificação do fabricante.

9.4.4 Cada módulo deverá estar certificado pelo fabricante.

9.4.5 Complementarmente, o adjudicatário promoverá a realização de sessões presenciais de esclarecimento, dirigidas aos técnicos do GRA, relativas à forma como as várias vertentes,



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

subsistemas e componentes que constituem a totalidade da solução adjudicada, foram implementadas, versando, designadamente, sobre:

- a) Subsistemas que integram a solução e respetivas componentes de hardware e software associadas a cada um;
- b) Função desempenhada por cada componente;
- c) Interações e interdependências entre os vários subsistemas/componentes;
- d) Modo de funcionamento de cada subsistema/componente;
- e) Pressupostos de configuração considerados em cada subsistema/componente;
- f) Parametrizações efetuadas em cada subsistema/componente;
- g) Alterações de implementação ocorridas face ao inicialmente planeado no serviço S1 e respetiva fundamentação;
- h) Recomendações relativas às políticas e procedimentos de utilização, administração, operação e manutenção da solução.

9.4.6 O concorrente deverá descrever detalhadamente, na sua proposta, os módulos de transferência de conhecimento necessários ao cumprimento dos objetivos descritos acima, bem como o conteúdo de cada um.

9.4.7 Os resultados da prestação deste serviço deverão ser documentados num relatório, designado por “Relatório R3 – Relatório de Formação”, que deverá incluir, no mínimo, a seguinte informação, relativa a cada módulo lecionado, para além de outras que o adjudicatário eventualmente entenda serem relevantes:

- a) Designação do módulo;
- b) Descrição sintética dos temas abordados;
- c) Locais, datas e horários de cada módulo;
- d) Lista de nomes dos participantes;
- e) Nome(s) do(s) técnico(s) do adjudicatário, responsáveis pela apresentação dos vários temas abordados e designação da respetiva empresa, caso se trate(m) de subcontratada(s).



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

9.5 Suporte a *software* e *firmware*

- 9.5.1 O adjudicatário garantirá a disponibilização *online* de *updates* e *upgrades*, para quaisquer componentes de *software* e *firmware*, relativos aos produtos integrados na solução, durante um período de três anos, a contar da data de aceitação provisória da solução.
- 9.5.2 Deverá ser assegurado o licenciamento de todas as componentes de hardware e software que integram a solução, sem prejuízo do estipulado no ponto anterior.
- 9.5.3 Quando solicitado, o adjudicatário prestará esclarecimentos técnicos sobre as funcionalidades disponibilizadas pela solução fornecida bem como sobre a forma como esta foi implementada no caso particular da entidade adjudicante.
- 9.5.4 Para efeitos do ponto anterior, a entidade adjudicante utilizará os canais indicados no ponto 10.1 de acordo com os níveis indicados na secção 11.

9.6 Apoio técnico do fabricante

- 9.6.1 Deverá ser disponibilizado um pacote com um mínimo de 100 horas de apoio técnico e com uma validade de utilização de 36 meses, a ser prestado diretamente pelo fabricante da solução fornecida, nos seguintes domínios:
- a) Alteração da configuração da solução durante o período de suporte;
 - b) Resposta a incidentes;
 - c) Investigação forense;
 - d) *Threat Intelligence*.

10 Condições de assistência na garantia

- 10.1 Os pedidos de assistência da entidade adjudicante deverão poder ser submetidos por esta, através de um sistema *online* de *ticketing* e uma linha de atendimento telefónico, em regime de 24 horas por dia, 7 dias por semana e 365 dias por ano, ambos disponibilizados pelo fabricante.
- 10.2 A resposta do adjudicatário aos pedidos de assistência, no âmbito da garantia, deverá ser assegurada de acordo com os níveis de serviço descritos na secção 11, devendo prioritariamente ser realizada uma intervenção remota para tentar diagnosticar e resolver o problema e, apenas se necessário, proceder a uma intervenção *on-site*.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 10.3 O número de pedidos de assistência permitidos deve ser ilimitado.
- 10.4 A entrega e recolha de quaisquer equipamentos de substituição do hardware em falha será *on-site*, com características equivalentes ou superiores, ficando a cargo do adjudicatário quaisquer encargos relacionados com essa operação.
- 10.5 A instalação de hardware de substituição, bem como a realização de quaisquer trabalhos de reparação local de hardware serão executados pelo adjudicatário que suportará os respetivos custos.
- 10.6 A instalação ou atualização de componentes de software, incluindo o respetivo licenciamento, com vista à resolução de problemas técnicos, ao abrigo da assistência na garantia, será executada pelo adjudicatário que suportará os respetivos custos.
- 10.7 Cada pedido de assistência formulado pela entidade adjudicante, independentemente do canal utilizado, deve ser objeto da criação de um ticket, através do qual deverão ser registados informaticamente todos os passos realizados até à resolução do problema e ao fecho do ticket. A entidade adjudicante deverá ter acesso a esse sistema (através de múltiplos utilizadores devidamente credenciados) e ser notificada, por e-mail, sempre que for criado um novo ticket ou quando o mesmo sofrer qualquer alteração de estado.

11 Níveis de serviço

- 11.1 A avaliação da qualidade dos serviços prestados será efetuada com base nas seguintes variáveis:
- a) Tempo de implementação – Número de dias de calendário despendidos para executar a implementação, assumindo-se que este culmina com o cumprimento das obrigações do adjudicatário necessárias e suficientes para a assinatura do auto de aceitação provisória;
 - b) Tempo de resposta (TR) – Tempo que decorre entre a comunicação da incidência de hardware/software pela entidade adjudicante e o início das ações de resolução pelo adjudicatário.
- 11.2 Quanto à variável “Tempo de resposta (TR)”, deverão ser considerados os seguintes graus de severidade:
- a) A (Crítica) – O componente encontra-se inoperacional ou numa condição que impossibilita a sua utilização efetiva (falha total ou quase total) e não existe



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

nenhum mecanismo de redundância instalado que permita assegurar as funções do componente em falha;

- b) B (Grave) – O componente encontra-se operacional, contudo a sua performance encontra-se seriamente afetada ou regista algumas falhas técnicas não impeditivas da sua utilização efetiva (falha parcial), ou ainda tenham sido detetadas falhas de parametrização que possam colocar seriamente em risco a qualidade dos serviços prestados ou a segurança das redes e dos sistemas informáticos do GRA. Alternativamente, o componente encontra-se inoperacional ou numa condição que impossibilita a sua utilização efetiva (falha total ou quase total), mas existem mecanismos de redundância instalados que permitem assegurar as funções do componente em falha;
- c) C (Menor) – O componente apresenta um ou mais problemas, mas sem impacto relevante na performance ou impedimento significativo na sua utilização efetiva;
- d) D (Regular) – A solução funciona com normalidade, estando em causa a solicitação de esclarecimentos ou correções a parametrizações que, embora não estejam em conformidade com as especificações deste Caderno de Encargos ou com as configurações que tenham sido acordadas com a entidade adjudicante durante a implementação, não apresentam risco elevado imediato para os sistemas do GRA.

11.3 Relativamente ao prazo para a aplicação de correções de parametrização que resultem de inconformidades com o estabelecido no Caderno de Encargos, nos casos em que seja necessário atuar, com carácter de urgência, face a situações que, mantidas no tempo, possam colocar seriamente em causa a qualidade dos serviços prestados ou a segurança das redes e dos sistemas informáticos do GRA, deverá aplicar-se o grau de severidade A, relativo ao tempo de resposta.

11.4 Quaisquer eventuais divergências entre as partes, quanto à atribuição do grau de severidade a um determinado incidente, serão tratadas de forma casuística, nos termos do presente Caderno de Encargos, da necessária concertação entre os contraentes e da legislação vigente.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 11.5 O adjudicatário deverá garantir o cumprimento dos níveis mínimos de serviço, apresentados no quadro seguinte, no que concerne à variável “Tempo de resposta (TR)”:

Quadro 1. Níveis de serviço a assegurar pelo adjudicatário.

Grau de severidade	Tempo de resposta (TR) máximo
A (Crítica)	1 hora
B (Grave)	2 horas
C (Menor)	4 horas
D (Regular)	Dia útil seguinte

12 Aplicação das sanções

- 12.1 O regime de sanções a aplicar, nos termos da Cláusula 27.^a, por incumprimento dos níveis de serviço respeitantes à alínea b) da secção 11.1, apenas será aplicável ao adjudicatário após a assinatura do auto de aceitação provisória da solução.
- 12.2 As sanções serão calculadas mensalmente pela entidade adjudicante e comunicadas ao adjudicatário, se esta entender que são aplicáveis. Caso este não conteste os cálculos apresentados no prazo de 8 dias úteis, a entidade adjudicante procederá à sua dedução nos termos do número 3 da Cláusula 27.^a.
- 12.3 O quadro seguinte sistematiza as sanções pecuniárias a aplicar em caso de incumprimento dos níveis de serviço, estabelecidos na secção 11, sendo P o valor a pagar para cada incidência.

Quadro 2 - Sanções a aplicar em caso de incumprimento dos níveis de serviço.

Situação de incumprimento	Base de Cálculo	Forma de Cálculo	Observações
Tempo de implementação superior ao estabelecido no número um da Cláusula 19. ^a	Uma só vez	$P = PD \times NDA$	PD – Sanção diária = 1/1000 do valor total de adjudicação, sem o IVA. NDA – N.º de dias de atraso, relativamente ao prazo proposto pelo adjudicatário.
Tempo de resposta (TR) superior ao estabelecido no quadro 1, acima indicado.	Por incidência	$P = PN \times NUTA$	PN – Sanção por cada unidade de tempo de atraso, conforme descrito no quadro 4, apresentado abaixo. NUTA – N.º de unidades de tempo de atraso, para cada grau de severidade, i.e., que excederam o tempo máximo contratado para a resposta à incidência. A unidade de tempo a utilizar será aquela que estiver associada ao grau de severidade da incidência, conforme descrito no quadro 3, apresentado abaixo.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- 12.4 Não haverá lugar a pagamentos ou devoluções ao adjudicatário, no caso de este exceder os requisitos estabelecidos pelas métricas.
- 12.5 O quadro seguinte sistematiza as unidades de contabilização do tempo de atraso associado a cada grau de severidade.

Quadro 3. Unidades de tempo de atraso, associadas a cada grau de severidade, relativamente aos valores do quadro 1.

Grau de severidade	Tempo de resposta (TR)
A (Crítica)	Hora
B (Grave)	Hora
C (Menor)	Hora
D (Regular)	Dia útil

- 12.6 Para efeitos do cálculo das sanções a aplicar, em caso de incumprimento dos níveis de serviço prescritos na secção 11, quaisquer tempos de atraso contabilizados serão arredondados às unidades superiores indicadas no quadro 3. Por exemplo, um atraso de 15 minutos numa intervenção *on-site*, relativamente ao grau de severidade A (correspondendo a 0,25 horas), será contabilizado como uma hora.
- 12.7 Os dias úteis serão contabilizados com base no calendário vigente na Região Autónoma dos Açores.

Quadro 4. Sanções a aplicar por unidade de tempo de atraso (em euros).

Grau de severidade	Tempo de resposta (TR)
A (Crítica)	100 (cem)
B (Grave)	
C (Menor)	
D (Regular)	



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

13 Organização e metodologia de execução

13.1 O concorrente deverá descrever detalhadamente, na sua proposta, a organização e a metodologia que se propõe utilizar para a execução do fornecimento da solução e dos serviços especificados neste Caderno de Encargos, devendo incluir a seguinte informação, para além de outros dados que considere relevantes:

- a) Plano de trabalho detalhado das atividades e tarefas a realizar;
- b) Cronograma de execução de todas as atividades e tarefas do projeto (diagrama de *Gantt*), incluindo aquelas que digam respeito à interação com a entidade adjudicante, ou que caibam a esta realizar;
- c) Caracterização da equipa de projeto do adjudicatário, indicando:
 - i. Estrutura funcional, com descrição das responsabilidades associadas a cada função;
 - ii. Indicação do número de recursos e respetivo perfil técnico, afetos a cada função;
 - iii. Na eventualidade de o concorrente proceder à subcontratação de outras empresas e/ou ter-se constituído como agrupamento de empresas, este deverá indicar quais as empresas que participam em cada bloco de trabalho, referido na alínea a) e quais as tarefas específicas atribuídas a cada uma.
- d) Metodologia de gestão do projeto, incluindo mecanismos de reporte à entidade adjudicante, sem prejuízo do estabelecido no presente Caderno de Encargos.

14 Qualificações e experiência do pessoal técnico

14.1 Os elementos da equipa encarregada da execução dos trabalhos objeto do presente Caderno de Encargos, deverão possuir qualificações técnicas adequadas à complexidade da solução e uma experiência profissional mínima de:

- a) Desempenho de funções, nos últimos cinco anos, equivalentes às que se propõem assumir no presente projeto;



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

- b) Participação técnica direta em, pelo menos, três projetos de tipologia e dimensão equiparáveis às do objeto deste procedimento, relativamente às vertentes em que será suposto intervirem.
- 14.2 O gestor de projeto, proposto pelo adjudicatário, deverá ter certificação válida, e reconhecida internacionalmente, na metodologia de gestão de projetos que pretende utilizar.
- 14.3 Após a comunicação da adjudicação, o adjudicatário deverá fazer prova de que os técnicos envolvidos na implementação e transferência de conhecimento da solução, possuem as competências e experiência adequadas, bem como certificações válidas e emitidas pelo fabricante, que garantam a sua qualificação para a realização dos trabalhos específicos em que estarão envolvidos.
- 14.4 Durante a execução do projeto, o adjudicatário apenas poderá proceder à substituição de elementos da sua equipa técnica com o exposto e prévio consentimento da entidade adjudicante, após verificação de que essa substituição proporciona um nível de qualidade equivalente.

15 Estrutura da proposta técnica

- 15.1 A proposta técnica a apresentar pelo concorrente deve ser dividida em duas partes:
- a) Parte I – Proposta;
- b) Parte II – Anexos.
- 15.2 A Parte I – Proposta deverá ser organizada em capítulos como se indica no quadro seguinte, cujo conteúdo deverá estar alinhado com a estrutura do Anexo A do Caderno de Encargos.

Quadro 5 - Estrutura e conteúdos da Parte I das propostas

Capítulo	Conteúdo
Capítulo 1 Sumário Executivo	Visão global da solução proposta em todas as suas vertentes, incluindo prazos, recursos e condições financeiras associadas.
Capítulo 2 Solução Técnica	Descrição pormenorizada da solução técnica proposta.
Capítulo 3 Serviços	Descrição pormenorizada dos serviços propostos, de acordo com o solicitado no Caderno de Encargos.
Capítulo 4 Organização e Metodologia de Execução	Descrição pormenorizada dos diversos aspetos organizativos que o concorrente propõe para assegurar a execução da implementação e a prestação da garantia e do serviço de suporte ao <i>hardware</i> e <i>firmware</i> .



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Capítulo	Conteúdo
Capítulo 5 Diversos	Descrição de outros aspetos e condições que o concorrente considere pertinente mencionar na sua proposta, não podendo, em circunstância alguma, contrariar os requisitos estabelecidos no Caderno de Encargos e no Programa do Concurso.
Capítulo 6 Matriz de Resposta a Ponto por Ponto	Neste capítulo deverá ser integral e detalhadamente preenchida a matriz de resposta ponto por ponto, conforme apresentada no Anexo B, cujo objetivo é de permitir ao concorrente fundamentar e comprovar que a sua proposta satisfaz, de facto, os requisitos do Caderno de Encargos.
Capítulo 7 Anexos	Índice com a identificação de todos os documentos anexos, apresentados na Parte II da proposta técnica, que deverão ser numerados sequencialmente para facilidade de referência (p.e., “01. Ficha técnica da sonda XPTO” ou “45. Lista de componentes”).

15.3 A Parte II – Anexos poderá ser constituída por uma pasta onde estejam localizados todos os documentos anexos.



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

ANEXO B – MATRIZ DE RESPOSTA A PONTO POR PONTO

O concorrente deverá preencher a matriz de resposta a ponto por ponto, apresentada abaixo, na sua totalidade, de forma objetiva e com o maior detalhe possível, para comprovar o cumprimento dos requisitos técnicos, constantes das secções 3 a 8 do Anexo A do Caderno de Encargos.

O fornecimento de informação parcial ou ambígua que não permita avaliar diretamente a conformidade da solução proposta com cada especificação do Caderno de Encargos, poderá impossibilitar a análise da proposta e a sua consequente exclusão do procedimento.

Na coluna “Síntese da solução que satisfaz o requisito e da respetiva fundamentação”, o concorrente deverá apresentar uma breve descrição clara e objetiva da solução proposta e da forma como esta permite satisfazer cada requisito específico indicado.

Na coluna “Fundamentação detalhada na proposta”, o concorrente deverá indicar a localização, na sua proposta, da fundamentação detalhada que comprove claramente que a solução proposta satisfaz integralmente o requisito em questão. Quando se trate da comprovação de funcionalidades ou atributos intrínsecos aos produtos propostos, o concorrente deverá anexar, à sua proposta, documentação e fichas técnicas do fabricante com indicação da posição exata da informação que confirma as respostas apresentadas (por exemplo, a ficha técnica NNNN do fabricante A respeitante ao produto B, na sua secção X, página Y, justifica o cumprimento do requisito Z do Caderno de Encargos).

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
3	Solução tecnológica pretendida	
3.1 a)		
3.1 b)		
3.1 c)		
3.1 d)		
3.1 e)		
3.2		
3.3		
3.4		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
3.5		
3.6		
3.7 a)		
3.7 b)		
3.7 c)		
3.7 d)		
3.8		
3.9 a)		
3.9 b)		
3.9 c)		
3.9 d)		
3.9 e)		
3.9 f)		
3.9 g)		
3.9 h)		
3.9 i)		
3.9 j)		
3.9 k)		
3.10		
4	Segurança dos endpoints	
4.1	Requisitos gerais	
4.1.1		
4.1.2 a)		
4.1.2 b)		
4.1.2 c)		
4.1.2 d)		
4.1.3		
4.1.4		
4.1.5		
4.1.6		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
4.1.7		
4.1.8		
4.1.9		
4.1.10		
4.1.11		
4.1.12		
4.1.13		
4.1.14		
4.1.15		
4.1.16		
4.1.17		
4.1.18		
4.2	Gestão	
4.2.1		
4.2.2		
4.2.3		
4.2.4		
4.2.5		
4.2.6		
4.2.7		
4.2.8		
4.3	Prevenção de Exploits	
4.3.1		
4.3.2		
4.3.3		
4.3.4		
4.3.5		
4.3.6		
4.3.7		
4.3.8		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
4.3.9		
4.3.10		
4.4	Prevenção de Malware	
4.4.1		
4.4.2		
4.4.3		
4.4.4		
4.4.5		
4.4.6		
4.4.7		
4.4.8		
4.4.9		
4.4.10		
4.4.11		
4.4.12		
4.4.13		
4.4.14		
4.4.15		
4.4.16		
4.4.17		
4.4.18		
4.4.19		
4.4.20		
4.4.21		
4.4.22		
4.4.23		
4.4.24		
4.4.25		
4.4.26		
4.4.27		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
4.4.28		
4.4.29		
4.4.30 a)		
4.4.30 b)		
4.4.30 c)		
4.4.30 d)		
4.4.30 e)		
4.4.30 f)		
4.4.30 g)		
4.4.30 h)		
4.4.30 i)		
4.4.30 j)		
5	SIEM (<i>Security information and event management</i>)	
5.1		
5.2		
5.3		
5.4		
5.5		
5.6		
5.7		
5.8		
5.9		
5.10		
5.11		
5.12		
5.13		
5.14		
5.15		
5.16 a)		
5.16 b)		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
5.16 c)		
5.16 d)		
5.16 e)		
5.16 f)		
5.16 g)		
5.16 h)		
5.17		
6	Análise de tráfego	
6.1	Sondas de tráfego	
6.1.1 a)		
6.1.1 b)		
6.1.1 c)		
6.1.1 d)		
6.1.1 e)		
6.1.2		
6.1.2 a)		
6.1.2 b)		
6.1.2 c)		
6.1.2 d)		
6.1.2 e)		
6.1.2 f)		
6.1.2 g)		
6.1.2 h)		
6.1.3		
6.1.4		
6.1.5		
6.1.6		
6.1.7		
6.1.8 a)		
6.1.8 b)		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
6.1.8 c)		
6.1.8 d)		
6.1.8 e)		
6.1.8 f)		
6.1.8 g)		
6.1.8 h)		
6.1.8 i)		
6.1.8 j)		
6.1.8 k)		
6.1.8 l)		
6.1.8 m)		
6.1.8 n)		
6.1.8 o)		
6.1.8 p)		
6.1.9		
6.2	Visibilidade sobre as máquinas	
6.2.1		
6.2.2 a)		
6.2.2 b)		
6.2.2 c)		
6.2.2 d)		
6.2.2 e)		
6.2.2 f)		
6.2.3		
6.2.4		
6.2.5		
6.3	Resposta a incidentes	
6.3.1		
6.3.2		
6.3.3		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
6.3.4		
6.3.5		
6.3.6		
6.3.7		
6.3.8		
6.3.9		
7	SOAR (Security Orchestration Automation and Response)	
7.1	Requisitos gerais	
7.1.1		
7.1.2		
7.1.3		
7.1.4		
7.1.5		
7.1.6		
7.1.7		
7.1.8		
7.1.9		
7.2	Arquitetura	
7.2.1		
7.2.2		
7.3	Playbooks	
7.3.1		
7.3.2		
7.3.3		
7.3.4		
7.3.5		
7.3.6		
7.3.7		
7.3.8		
7.3.9		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
7.3.10		
7.3.11		
7.3.12		
7.3.13		
7.3.14		
7.3.15		
7.3.16		
7.3.17		
7.3.18		
7.3.19		
7.3.20		
7.3.21		
7.3.22		
7.3.23		
7.4	REST API	
7.4.1		
7.5	Gestão de Incidentes	
7.5.1		
7.5.2		
7.5.3		
7.5.4		
7.5.5		
7.5.6		
7.5.7		
7.5.8		
7.5.9		
7.5.10		
7.5.11		
7.5.12		
7.5.13		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
7.5.14		
7.5.15		
7.6	Documentação	
7.6.1		
7.6.2		
7.6.3		
7.6.4		
7.6.5		
7.6.6		
7.6.7		
7.7	Colaboração	
7.7.1		
7.7.2		
7.7.3		
7.7.4		
7.7.5		
7.7.6		
7.8	Repositório de indicadores	
7.8.1		
7.8.2		
7.8.3		
7.8.4		
7.8.5		
7.8.6		
7.8.7		
7.9	Integração com ferramentas externas	
7.9.1		
7.9.2		
7.9.3		
7.9.4		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
7.9.5		
7.9.6		
7.9.7		
7.9.8		
7.9.9		
7.9.10		
7.9.11		
7.9.12		
7.9.13		
7.9.14		
7.10	Reporting	
7.10.1		
7.10.2		
7.10.3		
7.10.4		
7.10.5		
7.11	Machine Learning	
7.11.1		
7.11.2		
7.11.3		
7.11.4		
7.12	Updates	
7.12.1		
7.12.2		
7.13	Threat Intel Management (TIM)	
7.13.1		
7.13.2		
7.13.3		
7.13.4		
7.13.5		



REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO REGIONAL
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Referência do requisito no Caderno de Encargos	Descrição objetiva e sucinta da solução que satisfaz o requisito	Fundamentação detalhada na proposta (Indicar o capítulo, secção e os números de página na proposta, que permitam identificar a localização da fundamentação detalhada da resposta ao requisito)
7.13.6		
7.13.7		
7.13.8		
7.13.9		
7.13.10		
7.13.11		
7.13.12		
7.13.13		
8	Gestão de vulnerabilidades	
8.1		
8.2		
8.3		
8.4		
8.5 a)		
8.5 b)		
8.5 c)		
8.6		
8.7		
8.8		
8.9		
8.10		