



**REPÚBLICA
PORTUGUESA**

DEFESA NACIONAL

Aprovo.

Rui Manuel Alves Francisco

Comodoro

SECRETARIA-GERAL DO MINISTÉRIO DA DEFESA NACIONAL

Consulta Prévia

CADERNO DE ENCARGOS

AQUISIÇÃO DE SOLUÇÕES DE SEGURANÇA PARA ENDPOINTS E MOBILE

PARA A REDE DE DADOS DA DEFESA

Procedimento n.º 99/AP-UMC/2025



ÍNDICE

SECÇÃO I.....	4
DISPOSIÇÕES GERAIS	4
Cláusula 1. ^a - Entidade Adjudicante	4
Cláusula 2. ^a - Objecto do Procedimento	4
Cláusula 3. ^a - Anexos do Caderno de Encargos	5
Cláusula 4. ^a - Forma e documentos contratuais.....	5
Cláusula 5. ^a - Prazos	5
Cláusula 6. ^a - Local da prestação	6
SECÇÃO II	6
OBRIGAÇÕES CONTRATUAIS.....	6
SUBSECÇÃO I	6
OBRIGAÇÕES DO ADJUDICATÁRIO	6
Cláusula 7. ^a - Obrigações principais do adjudicatário.....	6
Cláusula 8. ^a - Meios Humanos e Materiais.....	6
Cláusula 9. ^a - Confidencialidade	7
Cláusula 10. ^a - Protecção de dados pessoais	7
Cláusula 11. ^a - Conflito de interesses e imparcialidade	8
Cláusula 12. ^a - Direitos de Autor e Responsabilidade pelo risco	8
SUBSECÇÃO II	8
OBRIGAÇÕES DA ENTIDADE ADJUDICANTE	8
Cláusula 13. ^a - Gestor do Contrato	8
Cláusula 14. ^a - Preço contratual	9
Cláusula 15. ^a - Preço Base	9



Cláusula 16. ^a	- Condições de pagamento	9
Cláusula 17. ^a	- Revisão de Preços.....	10
SECÇÃO III	10
PENALIDADES CONTRATUAIS E RESOLUÇÃO DO CONTRATO	10
Cláusula 22. ^a	- Penalidades.....	10
Cláusula 23. ^a	- Cessão da posição contratual	11
Cláusula 24. ^a	- Casos fortuitos ou de força maior	11
Cláusula 25. ^a	- Resolução do contrato	12
SECÇÃO IV	13
SEGURO DE RESPONSABILIDADE CIVIL	13
Cláusula 26. ^a	- Seguro de Responsabilidade Civil.....	13
SECÇÃO V	13
RESOLUÇÃO DE LITÍGIOS.....		13
Cláusula 27. ^a	- Foro competente.....	13
SECÇÃO VI	13
DISPOSIÇÕES FINAIS	13
Cláusula 28. ^a	- Contagem dos prazos.....	13
Cláusula 29. ^a	- Acompanhamento e Controlo Técnico	14
Cláusula 30. ^a	- Patentes, licenças e marcas registadas.....	14
Cláusula 31. ^a	- Configuração da execução do contrato.....	14
Cláusula 32. ^a	- Disposições e cláusulas por que se rege o fornecimento.....	15
Cláusula 33. ^a	- Comunicações e notificações	15
Cláusula 34. ^a	- Legislação aplicável	16
Cláusula 35. ^a	- Boa-fé	16
ANEXO II - ESPECIFICAÇÕES TÉCNICAS.....		17

SECÇÃO I
Disposições gerais**Cláusula 1.^a - Entidade Adjudicante**

- § A Entidade adjudicante é o Estado Português, através da Secretaria-Geral do Ministério da Defesa Nacional (SGMDN), com o NIPC: 600 032 205, com sede na Avenida Ilha da Madeira, 1 - 3.º Piso, 1400-204 Lisboa, telefone n.º 21 3010001, fax n.º 21 3020284, endereço de correio electrónico umcompras-mdn@defesa.pt, plataforma electrónica: www.acingov.pt.

Cláusula 2.^a - Objecto do Procedimento

1. O presente procedimento tem por objecto a aquisição de licenças para soluções de segurança para ENDPOINTS e MOBILE para a rede de dados da defesa, de acordo com as Especificações Técnicas, patentes no Anexo A do presente Caderno de Encargos e de acordo com as quantidades infra;

PART NUMBER	QTD	DESCRIÇÃO
Harmony Suite		
CP-HAR-EP-Advanced-1Y	950	Harmony Endpoint Advanced- Including Sandboxing, Web Protection, Attack Investigation, Threat Prevention, Access Control and Threat Intelligence, for 1 year
CP-HAR-EP-BASIC-1Y	320	Harmony Endpoint Basic- Including Web Protection, Attack Investigation, Threat Prevention, Access Control and Threat Intelligence, for 1 year
CP-HAR-MOBILE-DVC-1Y	75	Harmony Mobile, per-user single device subscription for 1 year

Cláusula 3.^a - Anexos do Caderno de Encargos

§ Faz parte integrante do presente CE os anexos seguintes:

- **Anexo A:** Especificações Técnicas

Cláusula 4.^a - Forma e documentos contratuais

1. O presente contrato reduzido a escrito, nos termos do n.º 1 do artigo 94.º do CCP, sendo composto pelo respectivo clausulado contratual e os seus anexos.
2. Fazem parte integrante do contrato os seguintes documentos:
 - Os suprimentos dos erros e das omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - Os esclarecimentos e as rectificações relativos ao caderno de encargos;
 - O presente caderno de encargos e respectivos anexos;
 - A proposta adjudicada;
 - Os esclarecimentos à proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos no número anterior, a prevalência é determinada pela ordem que nele se dispõe.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma legal.

Cláusula 5.^a - Prazos

§ As licenças das soluções de segurança para ENDPOINTS e MOBILE para a rede de dados da defesa deverão ser válidas por um período de 12 meses, com início a 1 de Abril de 2025.



Cláusula 6.^a - Local da prestação

- § As licenças das soluções de segurança, deverão ser entregues nas instalações da Secretaria-Geral do Ministério da Defesa Nacional, sitas na Av. Dr. Alfredo Bensaúde, 1849-014 Lisboa.

SECÇÃO II

Obrigações Contratuais

Subsecção I

Obrigações do adjudicatário

Cláusula 7.^a - Obrigações principais do adjudicatário

- § Sem prejuízo de outras obrigações previstas na legislação aplicável, decorrem para o adjudicatário todas as obrigações patentes CE, sob orientação e controlo da equipa interna do MDN.

Cláusula 8.^a - Meios Humanos e Materiais

1. O adjudicatário obriga-se a recorrer a todos os meios humanos e materiais que sejam necessários e adequados à execução do contrato.
2. São da exclusiva responsabilidade do adjudicatário as obrigações relativas ao pessoal por si utilizado na execução dos trabalhos, à sua aptidão profissional, à disciplina, à sua conduta, ao seu comportamento moral e à sua responsabilidade civil.
3. O adjudicatário deve possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato.
4. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da obtenção ou utilização, no âmbito do contrato, de patentes, licenças ou marcas registadas.



Cláusula 9.^a - Confidencialidade

1. Sem prejuízo do disposto no número seguinte, o adjudicatário compromete-se em guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao MDN, que lhe seja fornecida ou a que tenha acesso, relativa à execução do contrato ou em conexão com o mesmo, perdurando o dever de sigilo até dois anos após a cessação do contrato seja qual for a causa desta.
2. As partes só podem divulgar informações referidas no número anterior na medida em que tal seja estritamente necessário à execução do contrato, mediante autorização da parte que as haja prestado, ou do estritamente necessário ao exercício do direito de defesa em processo contencioso.
3. No caso previsto no número anterior, as partes devem garantir, em reciprocidade e em condições satisfatórias, a assunção, por escrito, de idêntico compromisso de confidencialidade pelos terceiros que acedam às informações abrangidas pelo dever de confidencialidade.
4. As partes devem ainda limitar o acesso às informações confidenciais aos seus quadros e funcionários que a elas tenham de recorrer para a correcta execução do contrato, assegurando que os mesmos são obrigados a manter essa confidencialidade.
5. São susceptíveis de serem consideradas informações confidenciais, sem prejuízo de outras que as partes decidam qualificar como tal, as que, a serem divulgadas, possam causar danos a qualquer das partes ou a terceiros, ou perturbar o normal desenvolvimento dos trabalhos da prestação de serviços objecto deste CE.
6. Os deveres referidos nos números anteriores abrangem igualmente as entidades subcontratadas pelo adjudicatário e a equipa técnica a afectar à presente aquisição.

Cláusula 10.^a - Protecção de dados pessoais

- 5 A actividade desenvolvida pelo adjudicatário e respectivos empregados ou colaboradores, no âmbito do presente procedimento, independentemente do vínculo contratual que possuam com o adjudicatário, encontra-se sujeito à aplicação do Regulamento Geral de Protecção de Dados (RGPD).



Cláusula 11.^a - Conflito de interesses e imparcialidade

1. O adjudicatário deve prosseguir a sua actividade de acordo com a lei aplicável e com as regras de boa-fé, tomando todas as medidas necessárias para evitar a ocorrência de quaisquer situações que possam resultar em conflito com os interesses da entidade adjudicante.
2. O adjudicatário obriga-se a não praticar qualquer acto ou omissão do qual possa resultar quaisquer ónus ou responsabilidades para a entidade adjudicante ou para os seus direitos e interesses.
3. O adjudicatário obriga-se ainda a suportar quaisquer encargos resultantes, designadamente, de reclamações, custos, despesas, multas, coimas ou sanções, necessários para a libertação de quaisquer ónus ou responsabilidades que recaiam sobre a propriedade da entidade adjudicante, quando tenham sido criados ou causados pelo adjudicatário ou por qualquer dos seus subcontratados.

Cláusula 12.^a - Direitos de Autor e Responsabilidade pelo risco

1. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, da prestação, de marcas registadas, patentes registadas ou licenças.
2. O adjudicatário será responsável e responderá até ao fim do contrato por todas as perdas e danos pessoais e/ou patrimoniais decorrentes da execução do contrato.
3. A entidade adjudicante será responsável pelos danos causados nos bens ou pessoal do adjudicatário ou de terceiros, quando estes tenham por origem negligência da sua parte.

Subsecção II

Obrigações da entidade adjudicante

Cláusula 13.^a - Gestor do Contrato

1. Nos termos do Artigo 290.º-A do CCP, por força do disposto na alínea i) do n.º 1 do artigo 96.º do mesmo código é nomeado um gestor de contrato.
2. O gestor do contrato da SGMDN acompanhará em permanência a sua execução.



Cláusula 14.^a - Preço contratual

1. Pela prestação dos serviços objecto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente CE, a SGMDN deverá pagar ao adjudicatário o preço da proposta adjudicada, acrescido do IVA à taxa legal em vigor. Os pagamentos serão trimestrais.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, incluindo as despesas de alojamento, alimentação e deslocação de meios humanos, quando aplicável.

Cláusula 15.^a - Preço Base

- § O preço base baseia-se na aquisição, em anos anteriores, de serviços de similares com o MDN. Neste sentido, o preço base cifra-se em **13 720,00 € (treze mil setecentos e vinte euros)**, ao qual acresce o IVA à taxa legal em vigor.

Cláusula 16.^a - Condições de pagamento

1. O pagamento do fornecimento objecto do presente procedimento é efectuado mensalmente, de acordo com a proposta financeira a apresentar, até trinta (30) dias após a data da recepção da factura, pela entidade adjudicante e após verificação dos formalismos legais em vigor para o processamento das despesas públicas.
2. A emissão da referida factura deverá ser processada após o fornecimento dos serviços pela entidade adjudicante, com todos os elementos justificativos do total apresentado.
3. A entidade adjudicante reserva-se no direito de não aprovar as facturas quando estas não respeitem o contrato ou o presente CE.
4. Na situação indicada no número anterior, a entidade adjudicante comunicará, a decisão ao adjudicatário que deverá apresentar outras facturas devidamente corrigidas em sua substituição.



Cláusula 17.^a - Revisão de Preços

- §** Não há lugar a revisão de preços durante a execução do contrato.

SECÇÃO III

Penalidades contratuais e resolução do contrato

Cláusula 22.^a - Penalidades

1. O incumprimento dos níveis de serviço e condições do fornecimento previstas no presente Caderno de Encargos confere à entidade adquirente o direito a ser indemnizada através da aplicação de uma sanção pecuniária, nos termos dos números seguintes.
2. Em caso de incumprimento do prazo fixado para o fornecimento nos termos previstos no presente Caderno de Encargos, por causa imputável ao adjudicatário, o mesmo fica sujeito, por cada dia de atraso, a uma penalidade de 1%, sobre o preço contratual, até ao limite acumulado de 20% do preço contratual.
3. As sanções previstas na presente cláusula não obstam ao eventual pedido de indemnização por parte da entidade adjudicante.
4. Nos casos em que seja atingido o limite previsto no n.º 2 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%.
5. O valor da sanção pecuniária a aplicar é creditado a favor da entidade adquirente ou deduzida ao preço a pagar pelo fornecimento.
6. Sempre que o adjudicatário não cumprir qualquer dos deveres a que se encontra vinculado, por razões imputáveis à entidade adjudicante, e que sejam por esta aceites como justificativos do incumprimento, não serão aplicadas as penalizações a que estaria obrigado em caso de incumprimento a si imputável.
7. A comunicação por escrito das razões imputáveis à entidade adjudicante, por parte do adjudicatário, será efectuada no prazo de 48 horas após a respectiva verificação, com a indicação da situação de incumprimento e respectivos fundamentos, presumindo-se a sua



aceitação caso não sejam contraditas no prazo de três dias, após a recepção da comunicação pela entidade adjudicante.

Cláusula 23.^a - Cessão da posição contratual

1. O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da entidade adjudicante.
2. Para efeitos da autorização prevista no número anterior, deve:
 - a) Ser apresentada pelo eventual cessionário toda a documentação exigida ao adjudicatário, nos termos previstos no convite;
 - b) A entidade adjudicante apreciar, designadamente, se o eventual cessionário não se encontra em nenhuma das situações previstas no artigo 55.º do CCP, e se tem capacidade técnica e financeira para assegurar o exacto e pontual cumprimento do contrato.

Cláusula 24.^a - Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior, for impedido de cumprir as obrigações assumidas no contrato.
2. Consideram-se como motivos de força maior, designadamente, os seguintes:
 - a) Epidemias supervenientes, greves, conflitos laborais, insurreições ou motins, guerra, invasão e mobilização que originem a suspensão ou interrupções do trabalho;
 - b) Movimentos sísmicos, incêndios, explosões, inundações e acidentes graves que suspendam ou interrompam o trabalho.
3. Não constituem casos de força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do adjudicatário 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 adjudicatário de deveres ou ónus que sobre ele recaiam;



- d) Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do adjudicatário 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 adjudicatário não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros.
4. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para o restabelecimento da situação.
5. Quando o motivo de força maior for reconhecido como comprovado pela entidade adjudicante, consideram-se os prazos acordados prorrogados pelo tempo em que aquele os tenha afectado.

Cláusula 25.^a - Resolução do contrato

1. O incumprimento dos deveres resultantes do contrato ou a prossecução deficiente do seu objecto por parte do adjudicatário constituirá fundamento de resolução imediata por parte da entidade adjudicante, sem que o adjudicatário tenha direito a qualquer indemnização.
2. O exercício do direito de resolução não prejudica o dever de indemnizar a entidade adjudicante pelos eventuais prejuízos resultantes das situações previstas no número anterior.
3. A resolução do contrato é notificada por correio sob registo e com aviso de recepção, produzindo efeitos a partir da data da respectiva notificação.
4. A cessação dos efeitos do contrato não prejudicará a verificação de responsabilidade civil ou criminal por actos ocorridos durante a execução da prestação objecto do presente procedimento.
5. Em caso de resolução ou suspensão do contrato, por qualquer título, o adjudicatário é obrigado a entregar de imediato toda a documentação e informação, independentemente da forma que esta revista, produzida no âmbito do contrato e que esteja em sua posse, a qual é, para todos os efeitos, propriedade exclusiva da entidade adjudicante.
6. O adjudicatário pode resolver o contrato por incumprimento grave e reiterado das obrigações contratuais por parte da entidade adjudicante, desde que tal incumprimento seja a esta



imputável, devendo notificar previamente a entidade adjudicante do motivo da resolução, no prazo máximo de 30 (trinta) dias úteis, a contar da data do conhecimento do facto, e dando-lhe um prazo não inferior a 60 (sessenta) dias úteis para sanar tal incumprimento.

7. Verificando-se a situação de resolução ou suspensão do contrato, por motivos não imputáveis ao adjudicatário, é devido a este o pagamento correspondente à fase em que se encontrem os trabalhos, na proporção directa dos dias efectivos de trabalho efectuado e aprovado, até à data da comunicação.

SECÇÃO IV

Seguro de Responsabilidade Civil

Cláusula 26.^a - Seguro de Responsabilidade Civil

- § Para cobrir eventuais danos, o adjudicatário deve garantir a validade pelo período abrangido pelo prazo de fornecimento de um Seguro de responsabilidade Civil para cobertura de danos causados pelo adjudicatário resultantes da execução de todas as tarefas decorrentes do fornecimento contratado.

SECÇÃO V

Resolução de litígios

Cláusula 27.^a - Foro competente

- § Para todas as questões emergentes do contrato, não solucionadas preferencialmente, dentro dos princípios da boa-fé contratual, para a resolução contenciosa das mesmas, será competente o Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

SECÇÃO VI

Disposições finais

Cláusula 28.^a - Contagem dos prazos



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

Cláusula 29.^a - Acompanhamento e Controlo Técnico

- § A entidade adjudicante pode aceder, livremente e a todo o momento, a qualquer documento que considere relevante para o acompanhamento dos trabalhos do adjudicatário.

Cláusula 30.^a - Patentes, licenças e marcas registadas

1. Serão da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, na execução do contrato, de marcas registadas, patentes registadas ou licenças.
2. Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, quaisquer dos direitos mencionados no número anterior, fica o adjudicatário obrigado a indemnizar aquela por todas as despesas que venham a resultar da referida demanda.

Cláusula 31.^a - Configuração da execução do contrato

A Secretaria-Geral do MDN é, exclusivamente, competente para, no âmbito do contrato, decidir sobre as seguintes matérias:

1. Revisões ou alterações ao contrato;
2. Levantamento do sigilo;
3. Cessão da posição contratual e admissão de subcontratação e contratação de tarefas;
4. Aplicação de penalidades;
5. Reconhecimento de casos fortuitos e força maior;
6. Aceitação de caução e exercício de quaisquer direitos a ela inerentes;
7. Rescisão do contrato e/ou negociações para reposição da situação de cumprimento.



Cláusula 32.^a - Disposições e cláusulas por que se rege o fornecimento

1. Na execução do objecto do presente procedimento observar-se-ão as cláusulas do contrato e o estabelecido em todos os documentos que dele fazem parte integrante.
2. Para os efeitos do estabelecido no número anterior, consideram-se integrados no contrato, em tudo quanto por ele não for explicitamente ou implicitamente contrariado, o Convite, o presente CE, bem como a proposta do adjudicatário e todos os outros documentos que sejam referidos no título contratual.
3. Na prossecução dos trâmites a seguir com vista à execução do objecto contratual, observar-se-á também o disposto:
 - a) No CCP, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de Janeiro, na sua redacção actual;
 - b) No Decreto-Lei n.º 252/94, de 20 de Outubro, na sua redacção actual;
 - c) Em mais legislação aplicável.
4. Em tudo o que o presente CE for omissivo ou suscitar dúvidas, aplicar-se-á a legislação em vigor em matéria de contratação pública.

Cláusula 33.^a - Comunicações e notificações

1. Em sede de execução contratual, todas as comunicações da entidade adjudicante dirigidas ao adjudicatário são efectuadas por escrito e enviadas através de correio registado ou correio electrónico.
2. As facturas deverão ser enviadas em formato digital para o endereço secretaria.geral@defesa.pt, ou através do Portal da Factura Electrónica na Administração Pública.
3. Em alternativa ao envio em formato digital, e desde que legalmente admissível, as facturas poderão ser remetidas para a Secretaria-Geral do MDN, sita em Av. Ilha da Madeira, n.º 1, 3.º Piso, 1400-204 Lisboa.



4. O adjudicatário deverá disponibilizar um relatório mensal, até ao décimo dia do mês seguinte, contendo as intervenções, recursos e tempos consumidos e tempos disponíveis.

Cláusula 34.^a - Legislação aplicável

1. O contrato que vier a ser celebrado fica sujeito à lei portuguesa, com renúncia expressa a qualquer outra.
2. Sem prejuízo de outras leis e regulamentos especialmente aplicáveis, a tudo o que não esteja expressamente previsto ou regulado no presente CE e na demais regulamentação do presente procedimento e do contrato, aplica-se o disposto no CCP.

Cláusula 35.^a - Boa-fé

5. As partes obrigam-se a actuar de boa-fé na execução do contrato e a não exercer os direitos nele previstos, ou na lei, de forma abusiva.



ANEXO A - ESPECIFICAÇÕES TÉCNICAS

(Documento anexo)

Especificação Funcional e Técnica

AQUISIÇÃO DE SOLUÇÕES DE SEGURANÇA PARA ENDPOINTS E MOBILE PARA A REDE DE DADOS DA DEFESA

Secretaria-Geral do Ministério da Defesa Nacional



GOVERNO DE
PORTUGAL

MINISTÉRIO DA DEFESA NACIONAL

Página deixada intencionalmente em branco

ÍNDICE

1. Introdução.....	7
1.1. Enquadramento	7
1.2. Organização do Documento	8
2. Informação / Documentação de Referência.....	9
2.1. Definição de Acrónimos, Abreviaturas e Simbologia.....	9
2.1.1. Lista de Acrónimos e Abreviaturas	9
2.1.2. Lista de Símbolos.....	10
2.2. Documentos de Referência	10
2.3. Organização dos Requisitos.....	10
3. Definição do Projeto.....	11
3.1. Antecedentes e Situação atual.....	11
3.2. Objetivos Gerais e Âmbito.....	12
3.3. Requisitos funcionais	12
3.4. Requisitos de Sustentabilidade	13
ANEXO A Características de Referência para as Soluções de segurança a Fornecer.....	14

Página deixada intencionalmente em branco

ÍNDICE DE TABELAS

Tabela 1 - Lista de Acrónimos e Abreviaturas	9
Tabela 2 - Lista com Documentos de Referência	10
Tabela 3 - Organização dos Requisitos	10

Página deixada intencionalmente em branco

1. INTRODUÇÃO

1.1. Enquadramento

A segurança de *endpoints* e *mobile* é uma área crucial da cibersegurança, focada na proteção de computadores (servidores, *desktops*, *tablets* e *smartphones*) e no seu acesso remoto seguro à rede corporativa com recurso a *Virtual Private Network* (VPN), contra ameaças externas e internas.

Proteger os *endpoints* é essencial para garantir a segurança dos dados, que podem ser comprometidos ou atacados por *malware*, *ransomware*, *phishing* e outros tipos de ciberameaças. Essa proteção pode incluir o uso de *firewalls*, antivírus, criptografia, autenticação multifatorial e políticas de segurança robustas para mitigar os riscos.

Com o aumento do trabalho remoto por trabalhadores internos e externos (fornecedores ou consultores) a prioridade deste tipo de segurança tornou-se mais pertinente para as organizações e indivíduos.

Os *endpoints* utilizados em trabalho remoto, representam um desafio adicional na segurança, pois são mais suscetíveis a perda, roubo ou acesso físico não autorizado. Se um dispositivo móvel for perdido ou roubado, os dados armazenados nele podem ser acedidos e explorados, direta ou indiretamente, por agentes maliciosos.

Além disso, muitos desses dispositivos podem ser conectados a redes Wi-Fi abertas e/ou inseguras e facilitar a intercetação de dados e ataques *Man-in-the-Middle* (MiTM). Não menos preocupante, são também os casos particulares dos acessos remotos pelos fornecedores e consultores com computadores próprios que estão fora do controlo de segurança do *endpoint* e potenciar sérios riscos adicionais.

Outro potencial risco prende-se com aplicações instaladas a partir de fontes não confiáveis que podem comprometer a segurança dos dispositivos móveis. Assim, torna-se imperativo restringir e monitorar os aplicativos instalados para garantir que não haja aplicativos maliciosos ou não autorizados de acordo com as políticas de segurança vigentes.

Num contexto de trabalho híbrido (presencial e remoto), a integração da segurança de *endpoints* com a segurança de dispositivos móveis é essencial. Muitas soluções de segurança incluem monitorização centralizada para dispositivos móveis e *endpoints*, permitindo uma resposta mais coordenada a incidentes de segurança. A combinação de proteção de dados, controle de acesso e visibilidade sobre os dispositivos é fundamental para manter a segurança num mundo digital cada vez mais móvel e conectado.

A segurança de *endpoints* e dispositivos móveis é desta forma uma componente essencial da estratégia de cibersegurança de qualquer organização. O avanço das tecnologias, a crescente dependência de dispositivos móveis e a digitalização do ambiente de trabalho tornam crucial a

implementação de soluções de segurança robustas, integráveis e práticas para proteger os dados, as redes e os sistemas de informação contra ciberameaças.

Face ao exposto, o presente documento visa definir Especificação Funcional e Técnica (EFT) para a aquisição de licenciamento de segurança de *endpoints* e *mobile*, para *upgrade* e substituição dos existentes que se encontram em multiplataformas e com prazo de licenciamento próximo de expirar ou renovar. Esta aquisição irá ter um impacto relevante, principalmente, no aumento da resiliência da Rede de Dados da Defesa da Secretaria-Geral do Ministério da Defesa Nacional (SGMDN), assim como dos sistemas de informação em exploração. Acresce sublinhar que esta ação irá também garantir uma substancial melhoria da cibersegurança das várias entidades do Ministério da Defesa Nacional (MDN).

1.2. Organização do Documento

Esta EFT está organizada da seguinte forma: no capítulo 2 é descrita a informação e/ou documentação de referência relevante para a presente aquisição; no capítulo 3 é efetuada a definição do projeto, com a enumeração dos objetivos e requisitos dos bens e serviços a fornecer.

2. INFORMAÇÃO / DOCUMENTAÇÃO DE REFERÊNCIA

Este capítulo estabelece a informação e documentação de referência relevantes para esta EFT.

2.1. Definição de Acrónimos, Abreviaturas e Simbologia

Esta secção identifica e define os acrónimos, abreviaturas, conceitos e simbologia relevantes e utilizados no contexto desta EFT.

2.1.1. Lista de Acrónimos e Abreviaturas

Esta subsecção identifica e define os acrónimos e abreviaturas relevantes e utilizados no contexto desta EFT.

A tabela seguinte apresenta a lista de acrónimos e abreviaturas:

Termo	Significado
BYOD	<i>Bring Your Own Device</i>
CCC	Centro de Comando e Controlo
CPU	<i>Central Processing Unit</i>
CDD	Centro de Dados da Defesa
DSCDD	Direção de Serviço do Centro de Dados da Defesa
EFT	Especificação Funcional e Técnica
EMM	<i>Enterprise Mobility Management</i>
IDS	<i>Intrusion Detection System</i>
IPS	<i>Intrusion Prevention System</i>
MFA	<i>Multi-Factor Authentication</i>
MDN	Ministério da Defesa Nacional
MiTM	<i>Man-in-the-Middle</i>
PDF	<i>Portable Document Format</i>
SGMDN	Secretaria-Geral do Ministério da Defesa Nacional
SMS	<i>Short Message Service</i>
SCCM	<i>System Center Configuration Manager</i>
SI	Sistemas de Informação
SIEM	Security Information and Event Management
SLA	<i>Service Level Agreement</i>
SO	Sistema Operativo
SSL	<i>Secure Sockets Layer</i>
URL	<i>Uniform Resource Locator</i>
VPN	<i>Virtual Private Network</i>

Tabela 1 - Lista de Acrónimos e Abreviaturas

2.1.2. Lista de Símbolos

Nada a mencionar.

2.2. Documentos de Referência

Nada a mencionar.

2.3. Organização dos Requisitos

Os requisitos descritos nesta EFT estão organizados da seguinte forma:

Id	Designação	Observações	Parágrafo
rFun	Requisitos Funcionais	Requisitos que estabelecem as características técnicas, funcionais e especificações operacionais.	3.3
rSus	Requisitos de Sustentabilidade	Requisitos que estabelecem as componentes necessárias à sustentação em operação da solução proposta (formação, documentação, garantia, etc.).	3.4

Tabela 2 - Organização dos Requisitos

3. DEFINIÇÃO DO PROJETO

3.1. Antecedentes e Situação atual

De acordo com a Portaria 290/2015, Artigo 9.º do DR n.º 183/2015, Série I de 2015-09-18, à Direção do Centro de Dados da Defesa (DSCDD), compete:

- a) Propor e acompanhar a implementação de soluções informáticas de apoio ao funcionamento da SGMDN ou necessárias à prossecução das suas atribuições;
- b) Garantir a operacionalidade e o desenvolvimento da infraestrutura tecnológica da SGMDN, designadamente ao nível das comunicações, dos equipamentos informáticos e dos suportes lógicos utilizados;
- c) Promover e assegurar o desenvolvimento, o aperfeiçoamento e a manutenção do Portal da Defesa, em articulação com as restantes unidades orgânicas da SGMDN;
- d) Assegurar os serviços de apoio aos utilizadores;
- e) Contribuir para o Plano de Ação Sectorial do MDN, enquanto plano estratégico para os Sistemas e Tecnologias de Informação do Ministério, incluindo o modelo de governação dos Sistemas de Informação (SI) da Defesa Nacional;
- f) Assegurar a prestação de serviços de tecnologias de informação e comunicação a todos os organismos da Defesa, no âmbito das atribuições previstas no modelo de governação dos SI da Defesa;
- g) Assegurar a administração da infraestrutura tecnológica partilhada que suporta os sistemas de informação de natureza comum;
- h) Assegurar a administração de sistemas aplicativos e de bases de dados da Defesa, no âmbito das atribuições previstas no modelo de governação dos SI da Defesa;
- i) Assegurar a administração da rede informática da Defesa, garantindo a sua adequada segurança, capacidade, disponibilidade, bem como a interoperabilidade e interconexão entre todos os serviços e organismos da área da Defesa e outras entidades nacionais e internacionais, no âmbito das atribuições previstas no modelo de governação dos SI da Defesa;
- j) Assegurar o apoio centralizado aos utilizadores dos SI de natureza comum.

Desta forma, nomeadamente na execução de medidas que visem essencialmente a garantia dos serviços de infraestruturas de segurança e comunicações, em articulação com as necessidades funcionais dos organismos utilizadores, torna-se essencial a existência de soluções de segurança para proteger os dados corporativos e pessoais, prevenir ataques cibernéticos e garantir a continuidade dos negócios. A proliferação de dispositivos móveis e o aumento do trabalho remoto tornam a segurança desses dispositivos ainda mais crucial. Investir em medidas como criptografia, autenticação forte, gestão de dispositivos, monitorização contínua é essencial para mitigar os riscos e garantir uma postura de segurança sólida.

Face ao exposto, identifica-se a necessidade de aquisição de licenciamento de soluções de segurança de *endpoints* e *mobile*, **por 12 meses**, integráveis com os sistemas de segurança de perímetro existentes, para *upgrade* e substituição dos existentes que se encontram em multiplataformas e com prazo de licenciamento próximo de expirar ou renovar.

3.2. Objetivos Gerais e Âmbito

- [OBJ-01] Integração com os *firewalls* de próxima geração existentes.
- [OBJ-02] Garantir a proteção de *endpoints*.
- [OBJ-03] Segurança de acesso remoto.
- [OBJ-04] Proteção para nuvem e infraestrutura.
- [OBJ-05] Gestão centralizada e visibilidade.
- [OBJ-06] Prevenção de ameaças em tempo real.
- [OBJ-07] Proteção para aplicações Web e móveis.
- [OBJ-08] Atender às normas e regulamentos de segurança.

3.3. Requisitos funcionais

(Gerais)

- [rFun-01] Integrar com *firewalls* de próxima geração da marca *CheckPoint*.
- [rFun-02] O concorrente deverá ser obrigatoriamente certificado pela marca fornecedora do produto, com o nível mínimo *Premier Partner*, ou equiparado. A certificação deve ser apresentada no momento da proposta, com data de vencimento seja superior à data de fim do presente contrato.

(Endpoints)

- [rFun-03] Detetar e impedir o *malware* no estágio de exploração, usando *Sandboxing* e Emulação em ambientes virtuais.
- [rFun-04] Executar o *malware* num ambiente seguro fornecendo uma forte proteção estática e dinâmica de primeira linha, usando assinaturas e análises comportamentais.
- [rFun-05] Bloquear proativamente a comunicação de Centros de Comando e Controlo (CCC) com o computador e interromper a exfiltração de dados.
- [rFun-06] Remediar a infeção de pelo menos duas maneiras: correção automática e correção manual.
- [rFun-07] Suportar fontes de inteligência adicionais de fornecedores externos.
- [rFun-08] Verificar os computadores quanto ao estado no nível do *patch* ou atualizações/*patches* específicos.

- [rFun-09] *Footprint* da solução com carga de CPU até 5%, consumo de memória até 300MB e uso de disco até 3GB.
- [rFun-10] Suportar os principais sistemas operativos, versões e computadores.
- [rFun-11] A solução deve ter *logging* que registre todas as ações de gestão.
- [rFun-12] Gerar alertas para administradores com base em eventos de *log* e fornecer granularidade total.
- [rFun-13] Fornecer a capacidade de bloquear ligações de/para serviços, portas e endereços IP específicos.
- [rFun-14] Registrar e/ou controlar o acesso a computadores removíveis com base num conjunto de regras especificadas e enviar as atividades ao servidor de gestão.

(Mobile)

- [rFun-15] Lidar com ameaças de diferentes vetores de ataque.
- [rFun-16] Detetar aplicações maliciosas conhecidos e desconhecidos, incluindo aplicações de risco.
- [rFun-17] Impedir o acesso a *links* maliciosos conhecidos do próprio dispositivo.
- [rFun-18] Evitar ataques de *phishing* e *zero-phishing*.
- [rFun-19] Bloquear e alertar sobre carregamento lateral.
- [rFun-20] Suportar a *Bring Your Own Device* (BYOD).
- [rFun-21] Suportar dispositivos móveis Android e iOS.
- [rFun-22] Fornecer avaliações completas de risco do dispositivo através de uma consola de gestão, nomeadamente o estado de risco dos dispositivos, o estado de proteção, os registos contínuos de eventos e alertas, assim como as opções de correção e mitigação no caso de ameaça real detetada.

3.4. Requisitos de Sustentabilidade

- [rSus-01] O fornecedor assegurar a prestação de garantia com assistência e suporte técnico, sem encargos para a SGMDN, com *Service Level Agreement* (SLA) de 8x5xNBD para todos os equipamentos pelo período do serviço solicitado. A proposta deverá discriminar os serviços de assistência técnica incluídos na garantia e que o adjudicatário se comprometerá a executar durante o respetivo período.
- [rSus-02] A solução fornecida, deverá incluir os manuais das soluções a fornecer, assim como os documentos de procedimento de instalação.

ANEXO A CARACTERÍSTICAS DE REFERÊNCIA PARA AS SOLUÇÕES DE SEGURANÇA A FORNECER

Características técnicas da solução de segurança dos *Endpoints*

1. Requisitos Gerais

a. A solução deverá ser capaz de detetar e impedir o *malware* no estágio de exploração, usando *Sandboxing* e Emulação em ambientes virtuais. Esta emulação deverá utilizar duas camadas de deteção de *exploits*:

- i. Tecnologia ao nível do *Central Processing Unit* (CPU) - Permite a deteção de explorações antes do *malware* ser executado;
- ii. Camadas de deteção adicionais que detetam comportamentos maliciosos e anómalos ao nível do Sistema Operativo (SO);
- iii. Ficheiros que contêm *exploits* são impedidos de fazer *download* para o computador. Se os ficheiros já estiverem no computador, os mesmos serão colocados em quarentena.

b. A solução deverá ser capaz de executar o *malware* num ambiente seguro fornecendo uma forte proteção estática e dinâmica de primeira linha, usando assinaturas e análises comportamentais. Utilizando a emulação de ameaças, que inclui tecnologias de deteção para identificar *malware* desconhecido para o qual não existem assinaturas. Deverá também fornecer uma camada adicional de prevenção de *malware* e ameaças, com uma proteção proativa de ameaças desconhecidas e de *zero-day*. A solução deverá suportar dois mecanismos principais de limpeza de ficheiros:

- i. Manter o tipo de ficheiro - entrega o ficheiro no seu formato original, removendo qualquer conteúdo ativo, como como macros;
- ii. Converter em *Portable Document Format* (PDF) - os arquivos entregues aos utilizadores devem ser convertidos para o formato PDF. O acesso ao ficheiro original deverá ser garantido apenas após emulação do mesmo num ambiente seguro.

c. A solução deverá ser capaz de bloquear proativamente a comunicação de CCC com o computador e interromper a exfiltração de dados. A comunicação com os CCC deverá ser identificada e bloqueada - evitando ações de *malware*, progresso de ataques e exfiltração de dados. Os processos que tentativa de comunicação com CCC devem ser encerradas e o executável colocado em quarentena. Os computadores identificados como infetados devem

ser isolados da rede - impedindo movimentos laterais, acesso a dados em servidores e comunicações CCC.

d. A solução deverá ser capaz de remediar a infeção de pelo menos duas maneiras: correção automática e correção manual. A correção deve incluir várias opções:

i. Quarentena de ficheiros maliciosos - a deteção pelos mecanismos de *Anti-Bot*, emulação de ameaças e *Anti-Ransomware* devem acionar a quarentena automática de ficheiros maliciosos;

ii. Remoção automática de *malware* - recurso automatizado de análise forense, que identifica todos os elementos de um ataque. Com base nessa análise, uma ação automatizada pode ser executada para remover todos os processos não respeitáveis que fazem parte do ataque. Também deve encerrar processos confiáveis que são usados de maneira maliciosa;

iii. Remoção de *malware* baseado em *script* - recurso automatizado de análise forense, que identifica todos os elementos de um ataque. Com base nessa análise, o produto pode gerar um *script* de remoção que pode ser usado em todos os *hosts* infetados para remover uma infeção generalizada. O *script* executa as mesmas ações que a opção de remoção automática de *malware*;

iv. Análise forense automatizada fornecida pelo produto deve permitir a correção refinada com base no entendimento profundo do ataque que é entregue pelo produto;

v. Análise forense automatizada, fornecida pelo produto, mostra o ponto exato de entrada. Ele deve permitir que o administrador reforce a segurança para impedir que o mesmo vetor seja bem-sucedido em ataques futuros.

e. A solução deve ter a capacidade de alavancar a inteligência em tempo real de bases de dados de ameaças alojadas numa nuvem comercial e/ou governamental (*hash*, assinatura, endereço IP, DNS, certificado digital e outros serviços de reputação) para detectar e/ou bloquear atividade maliciosa nos computadores. O produto deve suportar fontes de inteligência adicionais de fornecedores externos.

f. A solução deve verificar os computadores quanto ao estado no nível do *patch* ou atualizações/*patches* específicos. A componente de *compliance* deve ter a capacidade de verificar as configurações do registo na máquina local. Deve abranger atualizações e *patches* da *Microsoft* em várias versões do sistema operativo *Windows*.

g. A "*footprint*" da solução deve ter os seguintes requisitos:

i. O aumento da carga da CPU no intervalo de 0% a 5%;

- ii. O consumo de memória de até 300 MB;
- iii. O uso do disco é feito com as configurações padrão de até 3 GB.
- h. A solução deve suportar os seguintes sistemas operativos, versões e computadores:
 - ffff
 - i. Windows 7 32/64bit;
 - ii. Windows 8 32/64bit;
 - iii. Windows 8.1 32/64bit;
 - iv. Windows 10 32/64bit;
 - v. Windows 11 32/64bit;
 - vi. Windows 2008 R2 e todas as versões posteriores do servidores Windows;
 - vii. MacOS Big Sur 11;
 - viii. MacOS Catalina 10.15;
 - ix. MacOS Monterey 12;
 - x. MacOS Sequoia 15;
 - xi. MacOS Sonoma 14;
 - xii. MacOS Ventura 13;
 - xiii. Amazon Linux 2;
 - xiv. CentOS 7.8 - 8.5;
 - xv. Debian 9.12 - 11.8;
 - xvi. OpenSUSE 15.3, 42.3, 15.4-15.5;
 - xvii. Oracle Linux 7.9 - 8.8;
 - xviii. RHEL 7.8 - 8.9, 9.0-9.2, 9.3;
 - xix. SLES 12 SP5, 15 SP3;
 - xx. Ubuntu 16.04, 18.04, 20.04.
 - xxi. Alma Linux 8.9, 9.0-9.3;
 - xxii. Fedora 34-37, 38-39.
- i. A solução deve ter *logging* que registre todas as ações de gestão. Por exemplo: alterações na gestão de políticas, provisionamento de utilizadores e computadores, alterações de

administradores, *login/logout* de administrador, etc. Todas as deteções e proteções dos computadores devem ser registadas. Por exemplo: deteção e prevenção de *malware* por emulação/extração de ameaças, *Anti-Bot* (incluindo relatório completo), relatório de análise de ataque forense, ações de remediação e quarentena, etc.

j. A solução deve gerar alertas para administradores com base em eventos de *log* e fornecer granularidade total. Os alertas devem ter opção de ser configurados para serem enviados como notificação por *email* que pode gerar notificações de *push*, *Short Message Service (SMS)*, etc. O *logging* deve poder ser integrado com todos os principais produtos de *Security Information and Event Management (SIEM)*, que fornecem sua própria camada de alerta e granularidade. O produto também deve fornecer alertas aos utilizadores finais sobre qualquer infeção detetada.

k. A solução deve fornecer a capacidade de bloquear ligações de/para serviços, portas e endereços IP específicos numa base por processo ou função e fornecer as atividades ao servidor de gestão.

l. A solução deve registar e/ou controlar o acesso a computadores removíveis com base num conjunto de regras especificadas e enviar as atividades ao servidor de gestão. Deve fornecer controlo granular para periféricos e computadores de armazenamento. Todos os periféricos e acessos ao computador de armazenamento devem ser registados no sistema.

2. Administração Remota

a. A solução deve poder ser instalada e desinstalada manualmente. A instalação deve ser feita usando pacotes MSI. A desinstalação, deve ser protegida por autenticação de dois fatores (*Token*).

b. A solução deve permitir a instalação automática (instalador próprio, SCCM, EPO, etc.). A solução deve ser facilmente integrada com as ferramentas de instalação de terceiros, como o *System Center Configuration Manager (SCCM)*. A instalação alternativa pode ser feita via cliente de instalação inicial, que deve permitir instalações adicionais de *software* de acordo com a política definida.

c. A solução deve ter a opção de ser iniciada e parada remotamente. Os componentes de segurança relevantes devem ser removidos usando a opção de instalação de *software* ou desativados através da política.

d. A solução deve transferir *logs* de/para os computadores. Os *logs* devem poder ser extraídos usando a operação *push*. Essa funcionalidade deve ser controlada pela configuração da política.

- e. As atualizações da solução devem poder ser realizadas através da consola de gestão ou apenas por meio ferramentas de instalação de *software* para *desktop* (por exemplo, SCCM). As atualizações do cliente devem ser feitas utilizando os servidores de gestão ou usando pacotes de atualização com ferramentas de instalação de *software*, como o SCCM.
- f. A solução deve fornecer a capacidade de reverter para versões anteriores após correções e atualizações. A solução deve oferecer um mecanismo de gestão de *patches* do cliente que pode ser revertido a qualquer momento através de um processo autenticado.
- g. A solução deve ter proteção contra acessos e modificações não autorizadas/ mal-intencionadas, esta proteção deve ter tecnologia de autoproteção baseada em *kernel* incorporada.

3. Integração

- a. A solução deve fornecer integração com o *Splunk*, *McAfee Nitro* ou qualquer outro sistema SIEM. A exportação de dados para produtos externos deve ser feita via APIs OPSEC via *Syslog*.
- b. A solução deve fornecer integração aos sistemas de suporte técnico e sistemas de gestão de incidentes (por exemplo, JIRA, Remedy, ServiceNow etc.). A solução proposta deve poder integrar sistemas de *ticketing*.
- c. A solução deve poder proteger *downloads* efetuados na Internet antes de serem descarregados para o computador. A solução deve proteger proativamente os utilizadores em tempo real contra-ataques de *malware* avançados descarregados por meio de navegadores da Web. A solução deve permitir descarregar o ficheiro para o utilizador e entregar o conteúdo reconstruído e seguro em segundos, ao mesmo tempo deve enviar o ficheiro original para a análise e se o ficheiro for considerado seguro, o utilizador poderá fazer o *download* do ficheiro original sem a assistência do administrador ou do suporte técnico.
- d. A solução deve fornecer recursos anti-*phishing* e proteção de formulário da web. A solução deve poder bloquear o acesso a sites de *phishing*, bloqueando ataques de *phishing* desconhecidos e de *zero-day*, visando as credenciais do utilizador, verificando todos os campos do formulário e verificando a sua validade (isso deve ser feito em tempo real, com pouco ou nenhum efeito para a experiência do utilizador). A solução também deve alertar sobre a reutilização de senhas corporativas em sites externos.

4. Prevenção/Deteção de *Malware* & *Exploit*

- a. A solução deve proteger o sistema com as seguintes funcionalidades:

- i. Utilização de *sandboxing*/emulação, que monitoriza todas as atividades de *malware* e deteta a instalação do mesmo como parte da análise de *malware* resistente à evasão.
 - ii. O sistema de monitorização de ficheiros deve identificar um ficheiro gravado no sistema como parte da instalação do *malware* e deve enviá-lo para emulação.
 - iii. A instalação de *malware* geralmente inclui o *download* de *malware* adicional para comunicação com CCC. Esta comunicação deve ser detetada e bloqueada pelo *Anti-Bot*.
 - iv. Ficheiros maliciosos gravados durante o processo de instalação devem colocados em quarentena.
 - v. O recurso de análise forense automatizada deve identificar todas as etapas da instalação do *malware*, fornecendo um relatório destacando todos os elementos de *malware* instalados e adicionando um recurso para executar desinfecção precisa automaticamente.
 - vi. Anti-Virus deve detetar o *malware* usando a análise comportamental estática e dinâmica, cobrindo a instalação do *malware*.
 - vii. A entrega na forma de um documento deve ser higienizada com a Extração de ameaças - para que os utilizadores recebam ficheiros com o conteúdo enviado, mas sem os elementos maliciosos incorporados no conteúdo.
 - viii. A entrega na forma de executáveis deve ser tratada pela proteção de *Sandboxing*/Emulação de Ameaças para deteção avançada de ataques que não são baseados em assinaturas.
 - ix. Todos os elementos do ataque devem ser revelados após a análise forense automatizada.
- b. A solução deve ter uma deteção avançada baseada na emulação de ameaças, que deve utilizar vários métodos avançados de deteção que não são baseados em assinaturas. Algumas tecnologias devem incluir:
- i. Tecnologia ao nível do CPU - monitoriza o fluxo de execução dos programas ao nível do CPU, permitindo a deteção de *exploits* de *zero-day*, antes que qualquer código malicioso possa ser executado e, portanto, antes que a evasão possa ser tentada.
 - ii. Mecanismo de inteligência artificial - utilizado para análises estáticas e dinâmicas com base numa extensa plataforma de aprendizagem para deteção de *malware zero-day*.
 - iii. Mecanismo comportamental avançado - monitoriza vários indicadores de SO durante o tempo de execução.

c. A solução deve permitir uma extração de ameaças adotando uma abordagem proativa, fornecendo ficheiros higienizados aos utilizadores. Devem existir dois modos principais para esta abordagem:

i. Manter o formato do ficheiro - componentes ativos e potencialmente maliciosos, como macros, devem ser removidos do documento original. O ficheiro é reconstruído, simplificando a sua estrutura. A maioria dos ataques de *zero-day* devem poder ser evitados com essa abordagem.

ii. Converter em PDF - nesse modo, todos os documentos são convertidos em PDF antes da entrega. A extração de ameaças deve ser uma proteção prática que permite a entrega rápida de ficheiros aos utilizadores. Os utilizadores devem ter acesso automático e simples ao ficheiro original, caso precisem, mas somente depois que ele passar pelos mecanismos de Sandboxing/Emulação e se mostrar limpo.

d. A solução deve fornecer uma análise forense para analisar e revelar o ataque completo e as suas ameaças maliciosas ou interpretações suspeitas. Isso deve incluir a capacidade de rastrear os relacionamentos entre componentes de ataque, injeções de memória, etc. A análise deve ser realizada automaticamente ao longo de semanas e meses de atividade, abrangendo inicializações do sistema e rastreando processos de persistência de *malware*.

e. A solução deve ter a capacidade de impedir que tipos de *malware ransomware* e *cryptolocker* possam criptografar o sistema de ficheiros de um computador. Deve detetar o comportamento deste tipo de ataque, como excluir cópias de sombra, processos elevados das pastas temporárias, alterações nos registos MBR etc., descobrir essas ações deve acionar o *Anti-Ransomware* para bloquear a criptografia antes de ela começar.

f. Caso um *malware* do tipo *ransomware* ou *cryptolocker* tenha sido detetado e bloqueado após o início da criptografia, a solução deve recuperar os ficheiros criptografados para o estado pré-criptografado. Deve manter uma cópia protegida pelo *kernel* dos ficheiros do utilizador. Os ficheiros devem ser mantidos numa pasta segura que o *ransomware* não pode aceder.

g. A solução deve ter a capacidade de proteger um computador sem uma ligação constante à Internet. As seguintes funcionalidades devem ser garantidas:

i. A análise forense deve funcionar em todos os ambientes, independentemente da ligação de internet;

ii. Os recursos de deteção *Anti-Bot* baseados na inteligência devem poder funcionar em modo *offline*;

- iii. A emulação e a extração de ameaças devem poder ser executadas nos computadores *offline*;
- iv. A deteção, prevenção e restauração do *Anti-Ransomware* funciona deve funcionar em todos os ambientes, independentemente da ligação à Internet;
- v. Todas as ações de resposta (ficheiros de quarentena, bloqueio do computador ...) podem ser executadas quando *offline*.

5. Mitigação/Remediação

- a. A solução deve ter a capacidade de enviar ou receber atualizações de segurança, *patches*, conjuntos de regras sem assinatura, assinaturas, políticas e outros dados de configuração. Os clientes devem receber todas as informações relacionadas por meio de políticas e operações *push*.
- b. A solução deve ter a capacidade de fornecer informações forenses relacionadas o *malware* detetado. A análise forense deve incluir os acessos a ficheiros, chaves de registo confidenciais, criação de processos, modificação de registo/ficheiros, todas as comunicações de rede, atividade de *login* do utilizador, elevação de permissões, monitorização de variáveis de ambiente, etc.
- c. A solução deve ter a capacidade de executar verificações agendadas ou sob pedido por *malware* ou atividade maliciosa com base em assinaturas comerciais e/ou governamentais. O administrador deve poder usar o recurso de pesquisa e realizar uma verificação por qualquer indicador. Esta verificação deve resultar em análises forenses, quarentena de ficheiros, quarentena do computador, correção total do computador, etc. Esta verificação não deve deixar nenhum rastro significativo no computador.
- d. A solução deve ter a capacidade de colocar sistemas em quarentena automaticamente com base em regras personalizáveis (por exemplo, quando tipos de *malware* especificados são detetados). Devem ser utilizados os seguintes níveis:
 - i. Quarentena local no computador - usando Firewall incorporado no computador. Isso impedirá o computador de comunicar e atacar outros computadores ao seu redor.
 - ii. Quarentena usando *gateways*. A solução pode interagir automaticamente com as Gateways para implementar automaticamente a imposição nos computadores ofensivos. Além da quarentena do computador, há também a opção de automaticamente colocar em quarentena apenas o processo malicioso ou todos os processos que a análise forense decidiu que fazem parte do ataque.

e. A solução deve ter a capacidade de fornecer relatórios em tempo quase real de eventos específicos, com ações de resposta recomendadas para melhorar a segurança do *host*. Todos os incidentes de segurança devem ser totalmente analisados e o relatório resultante enviado quase em tempo real ao servidor de monitorização, incluindo informações altamente acionáveis, como análise do ponto de entrada, análise do impacto e todos os recursos maliciosos identificados no computador com base na atividade forense. Este relatório deve incluir informações detalhadas sobre o ponto de entrada no sistema, permitindo que o administrador identificar os pontos fracos de entrada e melhorar a política de segurança de acordo.

Características técnicas da solução de segurança de Mobile

1. Requisitos Gerais

- a. A solução deve lidar com ameaças de diferentes vetores de ataque - deteção de *malware*, ataques de *phishing*, links maliciosos, ameaças à rede e deteção de alterações nas explorações de SO e dispositivos, por forma a garantir que o dispositivo atenda à conformidade da política de segurança definida a nível empresarial.
- b. A solução deve detetar aplicações maliciosas conhecidos e desconhecidos, incluindo aplicações de risco (risco potencial se explorado, mas não prejudicial se usado com boas intenções).
- c. A solução deve impedir o acesso a *links* maliciosos conhecidos do próprio dispositivo.
- d. A solução deve evitar ataques de *phishing* e *zero-phishing*.
- e. A solução deve bloquear e alertar sobre carregamento lateral.
- f. A solução deve suportar a BYOD e dispositivos geridos/proprietários e corporativos.
- g. A solução deve suportar dispositivos móveis Android e iOS.
- h. A consola de gestão deverá fornecer avaliações completas de risco do dispositivo (correlacionar dispositivo, aplicativo e atividade da rede).
- i. A consola de gestão deverá fornecer ao administrador de segurança/SOC um painel visível para mostrar o estado de risco dos dispositivos, o estado de proteção e os registos contínuos de eventos e alertas.
- j. A consola de gestão deverá fornecer opções de correção e mitigação no caso de ameaça real detetada.

2. Requisitos de Deteção

- a. Deteção de *malware*:
 - i. Proteger aplicações maliciosos conhecidos e desconhecidos;
 - ii. Analisar o verdadeiro comportamento das aplicações;
 - iii. Deteção baseada na reputação do *developer* das aplicações;
 - iv. Permitir *whitelist* e *blacklist* de aplicações;
 - v. Atribuição inteligente do nível de gravidade às diferentes ameaças identificadas;
 - vi. Fornecer SLA padrão (hora) para detetar um *malware* desconhecido a partir do momento da instalação.

- b. Detecção de rede:
 - i. A solução deve detetar ligações comprometidas e tráfego de rede anómalo de e para o dispositivo (por exemplo, ataque MiTM);
 - ii. Detecção de intercetção *Secure Sockets Layer* (SSL) (striping SSL e SSL Bump);
 - iii. Capacidade de incluir na *whitelist*, certificados SSL conhecidos pela organização;
 - iv. Capacidade de definir a filtragem de *Uniform Resource Locator* (URL) e bloquear o acesso dos utilizadores quando o dispositivo estiver em risco;
 - v. Capacidade de bloquear o acesso a *links/phishing* maliciosos conhecidos e sites perigosos a partir do dispositivo;
 - vi. Fornecer navegação e mensagens seguras para impedir o acesso a *links* maliciosos.
- c. Explorações de SO e dispositivos:
 - i. A solução deverá detetar vulnerabilidades conhecidas e explorações de dispositivos;
 - ii. Detetar dispositivos com *jailbroken* e *rootkit*;
 - iii. Alerta sobre *Bluetooth exploits*;
 - iv. Detectar configurações arriscadas do sistema operativo;
 - v. Impedir mensagens de texto/SMS contendo *phishing* (AKA *Smishing*).
- d. Alerta para versões desatualizadas do SO.
- e. Capacidade de detecção de *anti-bot* para impedir que o *malware* aceda a sites maliciosos conhecidos, IPs e C&C.
- f. Bloquear a instalação do perfil de configuração do iOS com a capacidade de incluir na lista de permissões.
- g. Proteger no caso da aplicações com carregamento lateral:
 - i. Alerta no iOS da aprovação do certificado assinado pelo Enterprise/Developer que não está autorizado pela organização;
 - ii. Android - capacidade de forçar a verificação em qualquer distribuição de APK antes de ser instalada pelo utilizador e bloquear, caso o APK seja considerado malicioso;
 - iii. Bloquear o *download* do IPA ou do APK (baseado em políticas).
- h. Fornecer classificação de risco de dispositivo em pelo menos 3 níveis.
 - i. Detecção offline (opcional) - capacidade de detetar aplicações maliciosas carregadas no dispositivo quando offline.

j. A consola de gestão deve minimizar a deteção de falsos positivos (por exemplo, atribui baixo nível de risco a aplicativos válidos) - Característica importante para evitar casos de 'Cry Wolf' em ataques não prejudiciais.

3. Requisitos de Mitigação

a. A solução deve fornecer notificações ao utilizador e solicitar que o mesmo tome medidas, como excluir aplicações maliciosas, excluir mensagens de texto de *phishing* ou desconectar-se da rede hostil quando a ameaça for encontrada.

b. A solução deve integrar-se com *Unified Endpoint Management/Mobile Device Management/Enterprise Mobility Management* de terceiros, o que permite restrições para proteger *containers* ou fazer ajustes de política com base em riscos de dispositivos comprometidos (por exemplo, remoção de dados corporativos, dispositivo de quarentena, bloquear o acesso a recursos corporativos do dispositivo quando a ameaça for encontrada).

c. A solução deve integrar-se com soluções de *Container* para bloquear o acesso aos recursos corporativos quando o dispositivo for comprometido ou a solução de defesa contra ameaças móveis foi desinstalada.

d. A solução deve fornecer proteção de rede e mitigação de riscos para bloquear o acesso a sites maliciosos.

e. A solução deve impedir que o *malware* no dispositivo entre em contato com o CCC (*Anti Bot*).

f. A solução deve bloquear o acesso do dispositivo aos recursos corporativos (na *cloud* ou *on-Prem*) se o dispositivo estiver em risco, por exemplo. infetado com *malware* - Acesso condicional à rede do dispositivo.

g. A solução deve fornecer recursos de filtragem de URL, com base em categorias para impedir que os funcionários acessem sites não autorizados de acordo com a política da organização (por exemplo, impedir o acesso a conteúdo inadequado, como violência e jogos).

4. Requisitos Mobile Agent

a. A solução deverá suportar o sistema operativo mais recente de dispositivos móveis Android e iOS.

b. A solução deve suportar o cliente instalado via lojas oficiais Apple *AppStore/Google Play*.

- c. A solução dever alertar o utilizador sobre ameaças e fornecer ações de correção/mitigação por utilizador.
- d. A solução não deve permitir que o utilizador altere as configurações ou políticas de aplicações no seu dispositivo.
- e. A solução deve permitir o utilizador de ignorar alertas (configuráveis) - essa dispensa será registada nos *logs* como "ignorado pelo utilizador".
- f. A solução deve fornecer meios para garantir que a aplicação esteja em execução e protegendo o dispositivo (por exemplo, mecanismo para iniciar o aplicativo remotamente, executar em segundo plano ou ativar na inicialização do dispositivo).
- g. A solução deve ter suporte em vários idiomas para os locais de SO do dispositivo.

5. Visibilidade

- a. A solução deverá fornecer visibilidade e controlo completos dos eventos de segurança e do estado do dispositivo, com a capacidade de conduzir investigações detalhadas para garantir a aplicação de segurança das políticas móveis nos seguintes níveis:
 - i. SO/dispositivo;
 - ii. Apps;
 - iii. Rede.
- b. A solução deve integrar os eventos e alertas à solução SIEM (*send syslog/rsyslog*) e MDM/EMM para visibilidade do risco do dispositivo.
- c. A solução deve permitir a gestão e visibilidade completos dos riscos do dispositivo.

6. Gestão e Administração

- a. A solução deve utilizar uma consola de gestão centralizada.
- b. Acesso à consola de gestão - baseado na *Web* - nos principais *browsers*.
- c. A solução deve fornecer controlo de acesso baseado em função (funções de administrador).
- d. A solução deve permitir a configuração das políticas de segurança sem a necessidade de suporte avançado de codificação ou fornecedores. A política granular é necessária, pois utilizadores diferentes exigem configurações de segurança diferentes nos seus dispositivos móveis.
- e. Modelo de licenciamento deve ser simples - o modelo de licenciamento do produto:

- i. Ligação segura à consola (por exemplo, SSL);
 - ii. Capacidade de adicionar/remover dispositivos e agrupá-los;
 - iii. Os administradores podem criar o *email* de registo enviado aos utilizadores;
 - iv. Auditorias para ações de administração/uso;
 - v. Recursos de *login* único.
7. Funcionalidade de Relatórios e alertas
- a. Relatórios de estado do agente do dispositivo móvel:
 - i. Informações sobre quando foi a última ligação dos agentes para cada dispositivo;
 - ii. Informações sobre o estado de implementação do agente por dispositivo;
 - iii. Versão mais recente dos dispositivos;
 - iv. Número total de dispositivos instalados.
 - b. Elaborar relatório de risco:
 - i. Informações sobre riscos atuais que o sistema deteta;
 - ii. Informações sobre riscos do dispositivo por tipos;
 - iii. Capacidade de detalhar e investigar para obter mais detalhes sobre aplicações em risco.
 - c. Eventos e alertas:
 - i. Alertas de eventos de segurança distinguidos por tipo;
 - ii. Alertas de eventos de segurança em diferentes resoluções (a cada hora/diariamente /etc ..);
 - iii. Capacidade de enviar SMS e *emails* ao administrador para alertas de segurança;
 - iv. Relatórios de resumo agendados.