INSTITUTO DE INFORMÁTICA

CADERNO DE ENCARGOS

PROCESSO N.º 3001/20/0000213

RENOVAÇÃO DE SOLUÇÃO DE GESTÃO DE VULNERABILIDADES

Av. Prof. Dr. Cavaco Silva, 17 - Taguspark • 2740-120 Porto Salvo
Tel. + 351 214 230 000 • E-mail: ii@seg-social.pt • www.seg-social.pt

EFQM Recognised for Excellence 3 Star - 2017
EMPRESA CERTIFICADA eiC ISO/IEC 20000-1 APMG ISO/IEC 20000
EMPRESA CERTIFICADA eiC ISO/IEC 27001 certificação acreditada IAC

Capítulo I
Disposições Gerais

ARTIGO 1.º
OBJETO DO CONTRATO

O presente contrato tem por objeto a aquisição pelo **Contraente Público** de licenças perpétuas, atualizações e serviços no âmbito da gestão da solução de vulnerabilidades (Nexpose da Rapid7) ou equivalente, conforme discriminado no artigo 18.º e nos Anexos III e IV do presente caderno de encargos.

ARTIGO 2.º
CONTRATO

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2. O contrato a celebrar integra os seguintes elementos:
   a) Os suprimentos dos erros e das omissões do Caderno de Encargos identificados pelo Concorrente, 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 Caderno de Encargos;
   d) A proposta adjudicada; e
   e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

Capítulo II
Obrigações Contratuais
Secção I
Obrigações da Fornecedor
SUBSECÇÃO I
Disposições Gerais

ARTIGO 3.º
OBRIGAÇÕES PRINCIPAIS DO FORNECEDOR

Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o **Fornecedor** as seguintes obrigações principais:

a) Obrigação de entrega, instalação e configuração dos bens, bem como dos demais serviços identificados no caderno de encargos;
b) Obrigação de garantia dos bens;

c) Prestar os serviços afetando os recursos com os perfis solicitados, conforme exigido no artigo 18º do presente caderno de encargos e no Anexo III.

ARTIGO 4.º

CONFORMIDADE E OPERACIONALIDADE DOS BENS

1. O **Fornecedor** obriga-se a entregar ao **Contraente Público** os bens objeto do contrato com as características, especificações e requisitos técnicos 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 **Fornecedor** é responsável perante o **Contraente Público** por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

ARTIGO 5.º

ENTREGA DOS BENS

1. O **Fornecedor** obriga-se a entregar, instalar e configurar os bens objeto do contrato nas instalações sitas na sede do **Contraente Público**, no prazo de 10 dias a contar da celebração do contrato ou da comercialização, consoante o caso, nos dias úteis, entre as 9 e as 18 horas, salvo diferente determinação deste comunicada com a antecedência razoável.
2. O **Fornecedor** obriga-se a disponibilizar, simultaneamente com a entrega dos bens objeto do contrato, todos os documentos, em língua portuguesa, que sejam necessários para a boa e integral utilização ou funcionamento daqueles.
3. Com a entrega dos bens objeto do contrato, ocorre a transferência da posse e da propriedade daqueles para o **Contraente Público**.
4. Todas as despesas e custos com o transporte dos bens objeto do contrato e respetivos documentos para o local de entrega e com a respetiva instalação são da responsabilidade do **Fornecedor**.
5. O **Fornecedor** obriga-se a prestar os serviços de instalação de atualizações de acordo com as seguintes regras:
   a) O **Fornecedor** obriga-se a comunicar ao **Contraente Público** a comercialização das atualizações, no prazo de 5 dias a contar do evento;
   b) Os serviços serão prestados na sede do **Contraente Público,** nos dias úteis**,** das 9 horas às 17 horas**;**
   c) As tarefas serão planeadas e executadas de acordo com as prioridades definidas pelo **Contraente Público**;
   d) O **Fornecedor** deverá iniciar os trabalhos no prazo de 5 dias úteis, a contar da notificação do **Contraente Público** acompanhada da identificação dos trabalhos a realizar.

ARTIGO 6.º

INSPEÇÃO E TESTES

1. Efetuada a entrega do licenciamento e acesso de atualizações de software objeto do contrato, o **Contraente Público**, por si ou através de terceiro por ele designado, procede, no prazo de 15 dias, à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar, respetivamente, se correspondem às quantidades, características, especificações e requisitos técnicos e operacionais definido no presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.
2. A inspeção qualitativa a que se refere o número anterior é efetuada através dos testes.
3. Durante a fase realização de testes, o **Fornecedor** deve prestar ao **Contraente Público** toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar durante a realização daqueles, através de pessoas devidamente credenciadas para o efeito.

ARTIGO 7.º

INOPERACIONALIDADE, DEFEITOS OU DISCREPÂNCIAS

1. No caso de os testes previstos no artigo anterior não comprovarem a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos, o **Contraente Público** deve disso informar, por escrito, o **Fornecedor**.
2. No caso previsto no número anterior, o **Fornecedor** deve proceder, à sua custa e no prazo razoável que for determinado pelo **Contraente Público**, às reparações ou substituições necessárias para garantir a operacionalidade dos bens e o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
3. Após a realização das reparações ou substituições necessárias pelo **Fornecedor**, no prazo respetivo, o **Contraente Público** procede à realização de novos testes de aceitação, nos termos do artigo anterior.

ARTIGO 8.º

ACEITAÇÃO DOS BENS

1. Caso os testes a que se refere a artigo 6.º comprovem a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais, e neles não sejam detetados quaisquer defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos e na proposta, deve ser emitido, no prazo máximo de 15 dias a contar do final dos testes, um auto de receção, assinado pelos representantes do **Fornecedor** e do **Contraente Público**.
2. A assinatura do auto a que se refere o número anterior não implica a aceitação de eventuais defeitos ou de discrepâncias dos equipamentos objeto do contrato com as exigências legais ou com as características, especificações e requisitos técnicos.

ARTIGO 9.º

GARANTIA

1. Nos termos do presente artigo e da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, o **Fornecedor** garante o licenciamento contra quaisquer defeitos ou discrepâncias com as exigências legais e com características, especificações e requisitos técnicos definidos no presente Caderno de Encargos e na proposta.
2. No prazo máximo de dois meses a contar da data em que o **Contraente Público** tenha detetado qualquer defeito ou discrepância, este deve notificar o **Fornecedor**, para efeitos da respetiva reparação ou substituição.
3. A resolução dos problemas decorrentes de falhas deve ser realizada dentro de um prazo razoável fixado pelo **Contraente Público** e sem grave inconveniente para este último, tendo em conta a natureza do bem e o fim a que o mesmo se destina.
4. O **Cocontratante** obriga-se a prestar o suporte técnico decorrente de falhas provocadas pelo software ou pela sua instalação, de acordo com as seguintes regras e nos termos do **Anexo II**:
   - Gravidade de nível 1:
     - Resposta em 1 hora
     - Prestação ininterrupta (24x7)
   - Gravidade de nível 2:
     - Resposta em 4 horas
     - Prestação ininterrupta (24x7)
   - Gravidade de nível 3:
     - Resposta em 8 horas
     - Prestação das 9 horas às 18 horas, em dias úteis.

ARTIGO 10.º

FORMA DE EXECUÇÃO DO CONTRATO

1. Dada a natureza administrativa do contrato e a especial tecnicidade do respetivo âmbito**,** a execução será feita em estreita articulação com a equipa de projeto do **Contraente Público** e de acordo com as regras referidas no presente documento e nos artigos 303.º a 305.º do Código dos Contratos Públicos.
2. O **Fornecedor** obriga-se a comunicar ao **Contraente Público**, durante a execução do contrato, informações detalhadas sobre o funcionamento das atualizações.

ARTIGO 11.º

EXIGÊNCIA DE QUALIDADE

1. O **Fornecedor** obriga-se a executar os trabalhos de acordo com as normas e os princípios de qualidade pertinentes, bem como com as regras técnicas, a avaliar segundo o critério da melhor prática profissional, designadamente, no domínio das tecnologias de informação.

2. Em especial, o **Fornecedor** fica ainda obrigado a recorrer a todos os meios humanos e materiais que sejam necessários e adequados à execução do contrato, bem como ao estabelecimento do sistema de organização necessário à perfeita, completa e atempada execução das tarefas a seu cargo.

Subsecção II

Dever de sigilo e confidencialidade

ARTIGO 12.º

SIGILO E SEGURANÇA DA INFORMAÇÃO

1. O **Fornecedor** deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ou detida pelo **Contraente Público**, de que possa ter conhecimento ao abrigo do contrato, nos termos legalmente previstos, designadamente, no Regulamento Geral de Proteção de Dados e na legislação nacional que o execute, relativa à proteção de dados pessoais.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato;
3. Exclui-se do dever de sigilo, a informação e a documentação que o **Fornecedor** seja legalmente obrigada a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes;
4. Em especial, o **Fornecedor** obriga-se:
    a) A respeitar a confidencialidade sobre todos os dados disponibilizados pela ou pelas entidades envolvidas no projeto, bem como pelas informações de caráter pessoal ou processual dos beneficiários e contribuintes da Segurança Social, não os disponibilizando a quaisquer outras entidades; e
    b) Apagar ou destruir, no final do contrato, todo e qualquer tipo de registo (magnético ou em papel) relacionado com os dados pessoais tratados, bem como os que o **Contraente Público** considere como de acesso privilegiado.
5. De igual forma, o **Fornecedor** garante que terceiros que utilize na execução dos serviços respeitam os deveres referidos;
6. No âmbito das obrigações referidas no número anterior, o **Fornecedor** obriga-se a entregar ao **Contraente Público** cópias das declarações de sigilo assinadas pelos terceiros que utilize diretamente na execução do contrato, nos termos da minuta constante do **Anexo I** do presente caderno de encargos;
7. Os trabalhos e a utilização dos recursos pelo **Fornecedor** não se iniciarão antes da entrega das declarações de sigilo.

ARTIGO 13.º

PRAZO DO DEVER DE SIGILO

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

Secção II

Obrigações do Contraente Público

ARTIGO 14.º

PREÇO CONTRATUAL

1. Como contrapartida do fornecimento objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, o **Contraente Público** obriga-se a pagar ao **Fornecedor** o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço base é de 81 650,00 EUR (oitenta e um mil seiscentos e cinquenta euros), a que acresce o valor do IVA à taxa legal em vigor, distribuído da seguinte forma:
    a) Aquisição de 2.500 licenças – 35 675,00 EUR (trinta e cinco mil seiscentos e setenta e cinco euros);
    b) Atualizações de 2.500 licenças – 27 575,00 EUR (vinte e sete mil quinhentos e setenta e cinco euros);
    c) Serviços de operação e gestão para a quantidade máxima de 800 horas – 18 400,00 EUR (dezoito mil e quatrocentos euros)

ARTIGO 15.º

CONDIÇÕES DE PAGAMENTO

1. A(s) quantia(s) devidas pelo **Contraente Público**, nos termos do artigo anterior, deve(m) ser paga(s) no prazo de trinta dias após a receção da respetiva fatura, a qual só pode ser emitida com o vencimento da obrigação respetiva.
2. O pagamento do preço será efetuado da seguinte forma:
    a) Licenças, incluindo instalação e configuração, com a aceitação respetiva;
    b) Atualizações, em 4 prestações iguais, com vencimento a 60, 90 e 120 dias a contar da celebração do contrato e em outubro de 2021
    c) Serviços de operação e gestão da solução, após medição, de acordo com o registo de atividades semanais e indicando os recursos e o tempo afetos, a qual será comunicada ao **Contraente Público**, para validação prévia à emissão da respetiva fatura.

3. Em caso de discordância por parte do **Contraente Público**, quanto aos valores indicados nas faturas, deve este comunicar ao **Fornecedor** por escrito, os respetivos fundamentos, ficando esta obrigada a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. Para os efeitos do número 1, as obrigações só se vencerão se os bens e serviços tiverem sido aceites pelo **Contraente Público**.
5. Sob pena de devolução, a fatura deve ser explícita quanto ao objeto do contrato e incluir o n.º do pedido e compromisso a transmitir pelo **Contraente Público** aquando da celebração do contrato.

Capítulo III
Incumprimento

ARTIGO 16.º
PENALIDADES CONTRATUAIS

1. Nos casos de atraso no cumprimento das obrigações referidas no n.º 1 do artigo 5.º, n.º 2 do artigo 7.º e n.º 1.5 do artigo 18.º do caderno de encargos, por motivos imputáveis ao **Fornecedor** ou a terceiros que utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula P= Preço Contratual x A/100, em que P corresponde ao montante da penalização, e A é o número de dias de atraso.
2. Nos casos de atraso no cumprimento das obrigações previstas nos n.ºs 3 e 4 do artigo 9.º (Gravidade Nível 3) do presente caderno de encargos, por motivos imputáveis ao **Fornecedor** ou a terceiros que esta utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula P= Preço Contratual x A/500, em que P corresponde ao montante da penalização, e A é o número de horas de atraso, salvo se o prazo for fixado em dias, caso em que se aplica o número anterior.
3. Nos casos de atraso no cumprimento das obrigações previstas no n.º 4 do artigo 9.º do presente caderno de encargos (Gravidade Nível 1), por motivos imputáveis ao **Fornecedor** ou a terceiros que esta utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula P= Preço Contratual x A/100, em que P corresponde ao montante da penalização, e A é o número de horas de atraso, salvo se o prazo for fixado em dias, caso em que se aplica o número anterior.
4. Nos casos de atraso no cumprimento das obrigações previstas no n.º 4 do artigo 9.º do presente caderno de encargos (Gravidade Nível 2), por motivos imputáveis ao **Fornecedor** ou a terceiros que esta utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula P= Preço Contratual x A/200, em que P corresponde ao montante da penalização, e A é o número de horas de atraso, salvo se o prazo for fixado em dias, caso em que se aplica o número um anterior.
5. Considera-se de especial gravidade a violação pelo **Fornecedor** do dever de sigilo.

6. O atraso no pagamento do preço constitui o **Contraente Público** na obrigação de pagar juros à taxa legalmente devida.
7. Na determinação da gravidade do incumprimento, o **Contraente Público** tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do **Fornecedor** e as consequências do incumprimento.

ARTIGO 17.º

FORÇA MAIOR

1. Não podem ser impostas sanções ou exigidas indemnizações quando a não realização pontual das prestações contratuais a cargo de qualquer das partes resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
    a) Circunstâncias que não constituam força maior para os subcontratados do **Fornecedor**, na parte em que intervenham;
    b) Greves ou conflitos laborais limitados às sociedades do **Fornecedor** ou a grupos de sociedades em que esta se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
    c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo **Fornecedor** de deveres ou ónus que sobre ele recaiam;
    d) Manifestações populares devidas ao incumprimento pelo **Fornecedor** de normas legais;
    e) Incêndios ou inundações com origem nas instalações do **Fornecedor** cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
    f) Avarias nos sistemas informáticos ou mecânicos do **Fornecedor** não devidas a sabotagem;
    g) Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Capítulo IV

Cláusulas de conteúdo técnico

ARTIGO 18.º

SOFTWARE E SERVIÇOS A ADQUIRIR

1. <u>Descrição do objeto do contrato</u>

1.1. Aquisição das licenças de utilizador e serviços, abaixo descritos

Pos.	Designação	Quantidades
1	Aquisição de Licenças	2.500
2	Atualização de licenças	2.500
3	Serviços de operação e gestão da solução	Qt. máxima 800 horas
	Os requisitos técnicos para a prestação de serviços de operação e gestão da solução constam do **Anexo III**	
	As características da solução constam do **Anexo IV**	

1.2. A posição 1 do precedente 1.1., contempla a aquisição do licenciamento de software e acesso às atualizações do fabricante durante 12 meses, bem como, o serviço que visa assegurar a instalação e configuração da solução;

1.3. A posição 2 do precedente 1.1., contempla a aquisição das atualizações comercializadas e a comercializar no período compreendido entre 29 de outubro de 2020 e 28 de outubro de 2021;

1.4. Os serviços de operação e gestão da solução, referidos na posição 3 do precedente 1.1, deverão permitir a gestão, administração e operação da solução de vulnerabilidades e implementar a avaliação periódica do nível de segurança do Sistema de Informação da Segurança Social;

1.5. Os serviços de operação e gestão da solução serão realizados até 31 de dezembro de 2021, mediante notificação do **Contraente Público**, com a antecedência de 2 dias, contendo os trabalhos, as horas, o prazo e a data de início.

1.6. No caso de as licenças serem de outra solução que não a Nexpose da Rapid7, devem ser assegurados:

a) a conformidade com os requisitos técnicos mínimos ou superiores do Anexo IV;

b) a instalação, configuração e migração das configurações para a nova solução;

b) a passagem de informação aos técnicos do **Contraente Público**;

Capítulo V
Disposições finais

ARTIGO 19.º
TRABALHADORES

O adjudicatário obriga-se a cumprir com as obrigações decorrentes da legislação sobre trabalhadores estrangeiros, trabalho e segurança social.

ARTIGO 20.º
COMUNICAÇÕES E NOTIFICAÇÕES

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

ARTIGO 21.º
FORO COMPETENTE

As partes convencionam que todos os litígios emergentes do presente contrato serão resolvidos no foro administrativo da sede do **Contraente Público** com expressa renúncia a qualquer outro.

ARTIGO 22.º
CESSÃO DE CRÉDITOS

A cessão de créditos, designadamente no âmbito de contrato de "factoring" carece de autorização do **Contraente Público**

ARTIGO 23.º
CÓDIGO DE CONDUTA

O **Fornecedor** deve respeitar as regras consagradas no Código de Conduta de Fornecedores publicitado em www.seg-social.pt ("A Segurança Social" -> "Organismos" -> "Instituto de Informática, I.P." ->"Sistema de Gestão"->"Plano de Integridade e Transparência"), página 64 do Plano de Integridade e Transparência.

ARTIGO 24.º
INTEROPABILIDADE NA ADMINISTRAÇÃO PÚBLICA

O **Contraente Público** garante a utilização da plataforma de interoperabilidade da Administração Pública, sempre que seja conseguido esse acordo com as entidades com quem tenha de estabelecer, e se justifique, processos dessa natureza.

ARTIGO 25.º

LEGISLAÇÃO APLICÁVEL

São aplicáveis, em especial, ao presente contrato os Capítulos IV e V do Título I e Capítulos IV e V do Título II, da Parte III do Código dos Contratos Públicos.

ANEXO I
COMPROMISSO DE CONFIDENCIALIDADE

(Processo n.º 3001/20/0000213)

(minuta)

Entre:

EMPRESA e

xxxxxxxxxxx Trabalhador/Colaborador,

CONSIDERANDO QUE:

a) A **EMPRESA** vai fornecer bens que podem implicar a necessidade de aceder a informação ou a recursos de processamento de informação sob responsabilidade do Instituto de Informática, IP.;
b) O II, I.P. no exercício das suas atribuições tem acesso ou possui dados de natureza pessoal, técnica, económica ou financeira do sistema da Segurança Social que podem vir a ser conhecidos pela **EMPRESA** no fornecimento dos bens;
c) Se torna necessário proteger a confidencialidade desses dados;
d) O II, I.P. é detentor de elementos tecnológicos de base (Know-how e direitos de propriedade industrial e intelectual) nos quais assume a obrigação de manter a confidencialidade, obrigação essa que é extensível a todos os seus colaboradores ou outras pessoas que, de algum modo, possam ter acesso às informações transferidas;
e) O II, I.P., enquanto proprietário de múltiplos direitos sobre produtos resultado da investigação e desenvolvimento, pretende salvaguardar a confidencialidade dos mesmos para que possa, nomeadamente, assumir perante terceiros obrigações referentes aos seus próprios direitos;

é celebrado o acordo que consta das cláusulas seguintes:

Cláusula 1.ª

O Trabalhador/Colaborador obriga-se a:

a) Não divulgar nem fazer uso, de qualquer tipo e por qualquer meio, de toda a informação a que venha a ter acesso em virtude do vínculo que liga a **EMPRESA** ao II, I.P., salvo e na medida em que tal seja necessário para o exercício estrito das suas funções;
b) Manter sigilo sobre a organização, os métodos de trabalho, os negócios, as informações, os produtos, os materiais, os protótipos e sobre toda a documentação técnica que façam parte do Know-how, da propriedade ou estejam na posse dos serviços e organismos da Segurança Social, ou que a estes tenha sido cedido por terceiros;
c) Não fazer cópias de suportes magnéticos ou de manuais de produtos de software que pertençam ou que tenham sido facultados ao II, I.P. e aos serviços e organismos da Segurança Social, salvo se facultados

pela própria **EMPRESA** para uso não exclusivo do II, I.P. ou se para tanto obtiver uma autorização, formulada por escrito, pelo seu responsável direto.

Cláusula 2.ª

As obrigações assumidas nesta cláusula continuarão por um período de 10 anos após a extinção do contrato entre o II, I.P. e a **EMPRESA** sem prejuízo dos prazos de proteção dos direitos de propriedade intelectual ou outros legalmente fixados.

Lisboa, (dia) de (mês) de 202X

A Entidade Patronal

O Trabalhador/Colaborador

ANEXO II
NÍVEIS DE GRAVIDADE

Compete ao **Contraente Público** qualificar a gravidade dos incidentes ou problemas em função dos seguintes níveis:

Gravidade 1 (emergência)

- Paragem total ou parcial de qualquer das aplicações de suporte ao serviço;
- Impossibilidade de operação das plataformas ou indisponibilidade das suas interfaces de comunicação com o exterior da plataforma;
- Falhas de serviço, intermitentes ou não, que afetem a utilização do mesmo para um universo de utilizadores significativo;
- Falhas ou situações que elevem significativamente a probabilidade de ocorrência de uma quebra de serviço;
- Problemas que originem a utilização fraudulenta do serviço
- Falhas graves de alarmística de serviço ou plataforma

Gravidade 2 (problema crítico)

- Falha de redundância
- Falhas não graves de alarmística de serviço ou plataforma
- Falhas em facilidades da plataforma sem impacto nos clientes
- Falhas de serviço que sejam considerados como casos de utilizadores isolados, sem afetação geral.
- Falhas de produção de indicadores estatísticos

Gravidade 3 (problema não crítico)

- Situações de falha que não afetam o serviço, nem a normal operação.
- Falhas de documentação
- Esclarecimentos técnicos

ANEXO III

Requisitos técnicos para a prestação de serviços de operação e gestão da solução

1. Caracterização dos serviços a prestar

1.1. Os serviços de operação e gestão da solução compreendem:

a) Configuração e atualização da solução;
b) Configuração e implementação de scans de vulnerabilidades programados;
c) Criação de dashboards e indicadores da atividade;
d) Elaboração de relatórios periódicos de gestão e técnicos;
e) Apresentação da solução e passagem de conhecimento para as equipas técnicas;
f) Articulação de atividades com o CCO/SOC no âmbito da Gestão de Vulnerabilidades.

2. Recursos

2.1. A equipa técnica a alocar a este serviço deverá contemplar o perfil técnico, com as seguintes competências mínimas obrigatórias a comprovar pelo “curriculum vitae” e respetivas certificações:

a) Experiência mínima de 3 anos na instalação, configuração e operação do software Nexpose da Rapid7 ou equivalente;
b) Experiência mínima de 3 anos na implementação do software Nexpose da Rapid7 ou equivalente em ambientes iguais ou superiores a 5.000 ativos;
c) Certificação Nexpose Advanced Certified Administrator ou equivalente;
d) Conhecimentos de Linux;
e) Conhecimentos de Postgresql;
f) Capacidade de análise de dados CVSS;
g) Conhecimentos de arquitetura de redes.

ANEXO IV

Requisitos técnicos mínimos da solução

1. Arquitetura, desempenho e escalabilidade

1.1 – Possibilidade de utilizar elemento com função de gestão de vulnerabilidade que possa ser afixado em Rack padrão 19” ou que possa ser instalado em máquinas virtuais;

1.2 – Possuir scanner baseado em agentes;

1.3 – Possuir scanner baseado em Hardware ou em Máquinas Virtuais, suportando no mínimo:

- 1.3.1 – Vmware
- 1.3.2 – Hyper-V

1.4 – Permitir Scan em sistemas baseados em nuvem com scanners pré-aprovados, com suporte no mínimo a:

- 1.4.1 – Amazon AWS
- 1.4.2 – Microsoft Azure

1.5 – Gestão centralizada a partir de interface Web com acesso HTTPS;

1.6 – Permitir a criação de múltiplos níveis de utilizadores para administração da plataforma;

1.7 – Prevêr a utilização de duplo fator de autenticação para acesso à plataforma;

1.8 – Permitir a configuração de restrição de acesso à interface de gestão por meio do endereço IP de origem;

1.9 – Permitir fácil escalabilidade da solução, permitindo a ampliação do número de ativos detetados quando necessário;

1.10 – Permitir a configuração de perfis de desempenho dos scans, permitindo a escolha de quantidade de appliances utilizados e processos paralelos (mínimo 10);

1.11 – Realizar balanceamento de carga entre os scanner appliances para distribuição dos scans programados;

1.12 – Possuir dashboard configurável;

1.13 – A base deve ser atualizada de forma automática e constante, sempre que surgirem novas vulnerabilidades;

1.14 – O dispositivo scanner deve ser atualizado de forma automática, sem intervenção do operador;

1.15 – Dashboard com visualização de:

- 1.15.1 - Ameaças 0-Day;
- 1.15.2 - Vulnerabilidades sem patchs;
- 1.15.3 - Exploits/Vulnerabilidades mais facilmente exploráveis;
- 1.15.4 - Vulnerabilidades sem patchs disponibilizado pelo fabricante;
- 1.15.5 - Scans programados;

1.16 – Suporte a múltiplos utilizadores simultâneos.

2. Avaliação de Vulnerabilidade e Cobertura

2.1 – Permitir que sejam escolhidas as portas (TCP e UDP) que serão objeto de scan;

2.2 – Permitir a criação de filtros para deteção de vulnerabilidades específicas;

2.3 – Permitir que sejam realizados scans autenticados no mínimo em:

- 2.3.1 - Sistemas Windows
- 2.3.2 - Base de dados (Oracle, MySQL, Microsoft SQL Server, PostgreSQL)
- 2.3.3 - Sistemas baseados em UNIX
- 2.3.4 - HTTP
- 2.3.5 - SNMP
- 2.3.6 - Secure Shell (SSH)
- 2.3.7 - Secure Shell (SSH) Public Key
- 2.3.8 - File Transfer Protocol (FTP)
- 2.3.9 - Telnet
- 2.3.10 - Web Site Form Authentication
- 2.3.11 - Web Site Session Authentication

2.4 - Permitir a realização de "Força Bruta" em passwords em lista configurável, durante a execução do Scan.

2.5 - Tenha na sua base o mínimo 25000 (vinte e cinco mil) assinaturas;

2.6 - Permitir a configuração de scans de discovery (mapeamento):

- 2.6.1 – Fornecendo uma topologia básica dos ativos encontrados;
- 2.6.2 – Fornecendo informações sobre os sistemas operacionais detetados;
- 2.6.3 – Relatando a diferença entre scans realizados, mostrando novos ativos descobertos;
- 2.6.4 – Reportando os serviços em execução nos ativos no momento do scan;

2.7 – Permitir integração com ferramentas de SIEM de mercado;

2.8 – Possibilitar a realização de inventários de ativos;

2.9 – Habilidade para efetuar scan IPV4 e IPV6;

2.10 – Permitir Scan em sistemas por hostname e FQDN;

2.11 – Suporte a repositórios de passwords;

2.12 – Possibilidade de personalizar tabela de riscos por grupo de ativos;

2.13 – Permitir acesso aos relatórios e dados de scan por meio de REST API para integração com sistemas personalizados;

2.14 – Possibilidade de cancelar um scan enquanto este é executado;

2.15 – Permitir que os scans de mapeamento e de vulnerabilidade sejam agendados para execução automática e reiterada;

2.16 – Possibilitar que um agendamento pare automaticamente após número de execuções preestabelecido;

2.17 – Permitir o mapeamento dos ativos internos e externos (perímetro);

2.18 – Permitir que scans de vulnerabilidade sejam realizados tanto internamente como externamente (de acordo com os blocos de endereços definidos na RFC 1918);

2.19 – Deteção automatizada de Malware em Websites por meio de técnicas de análise comportamental e estatística;

2.20 – Suporte aos seguintes protocolos em análise de aplicações Web:

2.20.1 – HTTP 1.1

2.20.2 – HTTP 1.0

2.20.3 – SSL/TLS

2.20.4 – HTTP Keep-Alive

2.20.5 – HTTP compression

2.21 – Suporte aos seguintes esquemas de autenticação em análise Web:

2.21.1 – Basic;

2.21.2 – Digest;

2.21.3 – NTLM;

2.22 – Suporte a scans autenticados em aplicações Web:

2.22.1 – Baseado em formulário

2.22.2 – Automatizado, com a utilização de scripts

2.23 – Permitir a definição de URL como ponto de início do Scan;

2.24 – Suporte à submissão automática de formulários;

2.25 – Realizar o parsing em conteúdo Web para no mínimo:

2.25.1 – HTML

2.25.2 – JavaScript

2.25.3 – XML

2.25.4 – Texto puro

2.26 – Suporte às seguintes codificações de caracteres:

2.26.1 - ISO-8859-1

2.26.2 - UTF-7

2.26.3 - UTF-8

2.26.4 - UTF-16

2.27 – Conseguir identificar os seguintes problemas:

2.27.1 - Session token passed in URL

2.27.2 - Site supports weak SSL ciphers

2.27.3 - Reflected cross-site scripting

2.27.4 - Persistent cross-site scripting

2.27.5 - DOM-based cross-site scripting

2.27.6 - Cross-frame scripting

2.27.7 - HTML injection

2.27.8 - Cross-site request forgery

2.27.9 - OS command injection

2.27.10 - SQL injection

2.27.11 - HTTP header injection/response splitting

2.28 – Monitorizar o estado de certificados digitais, notificando sobre a sua expiração;

2.29 – Monitorizar e alertar sobre portas abertas que sejam identificadas nos scans;

2.30 – Alerta sobre vulnerabilidades críticas encontradas.

3. Conformidade e Gestão de Configurações

3.1 – Permitir a criação de políticas, com a utilização de controles pré-definidos;

3.2 – Permitir a configuração de controles personalizados para no mínimo:

3.2.1 – Sistemas baseados em UNIX:

3.2.1.1 – Verificação de existência de Arquivos/Diretórios;

3.2.1.2 – Verificação de permissões em Arquivos/Diretórios;

3.2.1.3 – Verificação de conteúdo de arquivos;

3.2.1.4 – Verificação de Integridade de arquivos;

3.2.2 – Sistemas Windows;

3.2.2.1 – Verificar existência de chaves de registo especificadas pelo utilizador;

3.2.2.2 – Verificar permissões de acesso em arquivos e diretórios;

3.2.2.3 – Verificar integridade de arquivos;

3.2.2.4 – Verificar permissões em arquivos;

3.2.2.5 – Verificar o conteúdo de valores em chaves de registo específicas;

3.2.2.6 – Verificar a existência de arquivos ou diretórios específicos;

3.2.3 – Possuir em sua base ao menos 6000 (seis mil) controles pré-definidos;

3.2.4 – Possibilitar a coleta de controles para criação de políticas a partir de hosts específicos (criação de baselines);

3.2.5 – Criar, controlar e reportar exceções sobre os controles e políticas;

3.2.6 – Possuir Dashboard configurável

3.2.7 – Possibilidade de mapear controles para os mais comuns frameworks como CIS, COBIT, HIPAA, ISSO 17799;

3.2.8 – Possibilidade de suportar controles para:

3.2.8.1 - Windows XP desktop

3.2.8.2 - Windows Vista

3.2.8.3 - Windows 7 e superior

3.2.8.4 - Windows 2012 Server

3.2.8.5 - Windows 2008 Server

3.2.8.6 - Windows 2008 Active Directory

3.2.8.7 - Windows 2003 Server

3.2.8.8 - Windows 2003 Active Directory

3.2.8.9 - Windows 2000 Active Directory

3.2.8.10 - Windows 2000

3.2.8.11 - Ubuntu 8.x ou superior
3.2.8.12 - Solaris 9.x ou supeior
3.2.8.13 - Red Hat Enterprise Linux 3 ou superior
3.2.8.14 - Oracle Enterprise Linux 4.x ou superior
3.2.8.15 - Oracle 9i
3.2.8.16 - Oracle 10g ou superior
3.2.8.17 - Microsoft SQL Server 2012
3.2.8.18 - Microsoft SQL Server 2008
3.2.8.19 - Microsoft SQL Server 2005
3.2.8.20 - Microsoft SQL Server 2000
3.2.8.21 - MS IIS 7.x
3.2.8.22 - MS IIS 6.0 Cisco IOS 15.x
3.2.8.23 - Cisco IOS 12.x
3.2.8.24 - CentOS 4.x ou supeior
3.2.8.25 - Apache HTTP Server 2.2.x

4. Registo e Controlo das vulnerabilidades

4.1 – Fornecer, integrado ao sistema de gestão de vulnerabilidades, ferramenta para controle individual de cada uma das vulnerabilidades apresentadas nos elementos da rede;
4.2 – Permitir a definição de regras com critérios personalizáveis para a abertura de tickets e direcionamento destes para um grupo de utilizadores pré-definido;
4.3 – Permitir redirecionar um ticket de um utilizador para outro;
4.4 – Possibilitar, quando configurado, que um ticket seja encerrado pela plataforma somente após confirmado por esta que a vulnerabilidade já não está presente neste sistema;
4.5 – Permitir, quando permitido, que um utilizador encerre um ticket em aberto;
4.6 – Permitir a definição de período máximo que um ticket deve ser tratado, alertando quando este período ultrapassar o configurado;
4.7 – Permitir o envio automatizado de e-mails de notificação pela plataforma
4.8 - Integração com ferramentas de ITSM de mercado (preferencial Easyvista).

5. Relatórios

5.1 – A plataforma deve permitir que os relatórios sejam gerados, visualizados e armazenados de forma centralizada;
5.2 – Deve possuir a possibilidade de partilha de relatórios de forma automatizada por meio de emails a partir da plataforma;
5.3 – Expirar relatórios automaticamente para liberar espaço no repositório para novos relatórios;
5.4 – Permitir a distribuição automatizada de relatórios criptografados no formato PDF;
5.5 – Possuir templates pré-configurados para a execução de relatórios de gestão e técnicos;

5.6 – Capacidade para executar os relatórios para se obter o resultado de hosts/devices especificados;

5.7 – Deve possuir capacidade para que novos templates sejam configurados conforme a necessidade do utilizador da plataforma no mínimo com as seguintes informações:

5.7.1 – Informações baseadas em tendências

5.7.2 – Gráficos para no mínimo:

5.7.2.1 – Portas detetadas;

5.7.2.2 – Vulnerabilidades por Severidade

5.7.2.3 – Sistemas Operacionais Detetados

5.7.2.4 – TOP 10 Vulnerabilidades

5.7.3 – Incluir detalhes sobre as vulnerabilidades encontradas;

5.7.4 – Soluções para as vulnerabilidades encontradas;

5.8 – Capacidade para filtrar vulnerabilidades específicas do relatório;

5.9 – Possibilidade de filtrar vulnerabilidades que não sejam exploráveis

5.10 – Possibilidade de selecionar níveis específicos de vulnerabilidades nos relatórios (por nível de severidade);

5.11 – Opção para relatórios de Patchs a serem aplicados;

5.12 – Scorecard reports;

5.13 – Relatórios específicos para remediação das vulnerabilidades encontradas;

5.14 – Relatórios devem ser exportados no mínimo nos seguintes formatos:

5.14.1 – PDF

5.14.2 – XML

5.14.3 – CSV

5.14.4 – HTML

5.14.5 – MHT

5.15 – Permitir a extração de relatórios para o módulo de remediação;

5.16 – Extração de relatórios de Compliance para aplicações Web (OWASP);

5.17 – Sobre as vulnerabilidades, deve informar:

5.17.1 – Descrição da vulnerabilidade

5.17.2 – CVE

5.17.3 – Nível de criticidade

5.17.4 – Guia para remediação

6. Proteção contra ameaças e inventario de ativos

6.1 – Deverá comparar dados de ameaças externas com relação das vulnerabilidades internas da organização independentemente de sua vertical e permitir a priorização no trabalho de correção como implementação de patchs e redução de riscos.

6.2 – Identificar ativos com maior risco, através de feeds de informações contra ameaças em tempo real com mecanismo de pesquisa em tempo real, afim de procurar ativos que possuem determinada vulnerabilidade.

6.3 – Fornecer mecanismo de pesquisa em tempo real capaz de identificar um ou mais itens abaixo dentro do ambiente correlacionado com a mesma consola de gestão das vulnerabilidades:

6.3.1 – Softwares instalados e versões;

6.3.2 – Serviços ativos;

6.3.3 – Portas abertas;

6.3.4 – Hostname;

6.3.5 – Vulnerabilidades e exploits públicos caso existem;

6.3.6 – Zero Days (Vulnerabilidades sem correção);

6.3.7 – Hosts com Vulnerabilidades com exploit;

6.3.8 – Hosts com Vulnerabilidades em patch disponível;

6.3.9 – Vulnerabilidades ligadas a extração de dados;

6.3.10 – Vulnerabilidades ligadas a malwares populares;

6.4 – Fornecer todo o inventário do parque podendo usar scans virtuais autenticados ou agentes para alimentar diariamente a base de dados;

6.5 – Permitir que sejam feitas pesquisas no ambiente, através de informações na base de dados utilizando tecnologia de pesquisa similar à pesquisa do Google;

6.6 – Possibilidade de possuir diversos dashboads dinâmicos com widgets dinâmicos conforme as informações são atualizadas.