

## **Contrato 24/IFAP/060**

Entre:

**IFAP - Instituto de Financiamento da Agricultura e Pescas, I.P.** com sede na Rua Castilho, n.º 45 a 51, em Lisboa, pessoa coletiva n.º 508 136 644, neste ato representado pelo Eng. Rui Manuel Costa Martinho., Presidente do Conselho Diretivo, nomeado pelo Despacho n.º 8630/2023, de 18 de Agosto de 2023, publicado no Diário da República n.º 165, 3.º II Série, de 25 de Agosto de 2023, adiante designado por IFAP, I.P., como Primeiro Outorgante;

e

**RELOAD-Consultoria Informática, Unipessoal Lda.**, com sede na Rua Monte da Bela, 181W, 4445-294 Ermesinde, pessoa coletiva n.º 506 210 855, neste ato representada por Miguel Angel Simões Santiago, na qualidade de representante legal, com poderes para outorgar o presente contrato, conforme documento comprovativo que exibiu, como Segundo Outorgante;

### **E CONSIDERANDO QUE:**

1. A despesa foi autorizada por Deliberação do Conselho Directivo do IFAP, I.P., de 26 de Dezembro de 2024, ao abrigo da competência nele delegada pelo disposto nos termos do disposto no n.º 3 do artigo 38.º da Lei Quadro dos Institutos Públicos, aprovada pela Lei n.º 3/2004, de 15 de Janeiro, e será suportada pela dotação orçamental inscrita no orçamento de funcionamento do IFAP, I.P.;
2. O fornecimento de bens e a prestação de serviços foi adjudicado por Deliberação do Conselho Directivo do IFAP, I.P., de 24 de Dezembro de 2024, no uso das competências delegadas pela deliberação referida na alínea anterior;
3. A minuta do presente contrato foi aprovada pela referida deliberação no uso das referidas competências;

É celebrado e reciprocamente aceite o presente contrato relativo ao , o qual se regerá pelas cláusulas seguintes:

Cláusula 1.<sup>a</sup>

**(Objeto)**

O objeto do contrato consiste no seguinte:

- Substituição e manutenção de firewalls, para os anos de 2025, 2026 e 2027

Tendo em atenção as especificidades e as características técnicas dos bens e dos serviços a adquirir definidas no Anexo I ao presente contrato.

Cláusula 2.<sup>a</sup>

**(Gestor do Contrato)**

O primeiro outorgante designa como gestores do contrato pela sua parte, nos termos do previsto no número 1 do Artigo 290.º -A do Decreto-Lei n.º 111-B/2017, de 31 de Agosto, o colaboradore seguinte:

- [REDACTED]

Cláusula 3.<sup>a</sup>

**(Prazo de vigência)**

O contrato inicia a respetiva produção de efeitos a 08 de Junho de 2025 e cessa a sua vigência, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação, a 07 de Junho de 2028, mantendo-se as obrigações acessórias que devam perdurar para além do seu termo.

Cláusula 4.<sup>a</sup>

**(Conformidade dos bens e serviços)**

1. O Segundo Outorgante obriga-se, perante o Primeiro Outorgante, a entregar-lhe os bens e prestar-lhe os serviços objecto do contrato a celebrar, em conformidade com as especificações do presente contrato.
2. Os bens objecto 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 ao seu funcionamento.

3. É aplicável, com as necessárias adaptações, aos bens a adquirir e aos serviços a prestar no âmbito do contrato a celebrar, o disposto na lei que disciplina os aspectos relativos à venda de bens de consumo, à prestação de serviços e às garantias a elas relativas, no que respeita à responsabilidade e às obrigações do fornecedor do produto, do prestador de serviços e aos direitos do consumidor.
4. O Segundo Outorgante é responsável, perante o Primeiro Outorgante, por qualquer defeito ou discrepância dos bens ou por qualquer problema ou discrepância dos serviços objecto do presente contrato, que se verifiquem, respectivamente, no momento em que os bens lhe são entregues ou os serviços lhe são prestados.

Cláusula 5.<sup>a</sup>

**(Documentos contratuais)**

1. Fazem parte integrante do contrato os seguintes documentos:
  - a) Os suprimimentos dos erros e omissões do caderno de encargos identificados pelas entidades concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
  - b) Os esclarecimentos e as rectificações relativas ao caderno de encargos;
  - c) O caderno de encargos;
  - d) A proposta adjudicada;
  - e) Os esclarecimentos à proposta adjudicada prestados pelo Segundo Outorgante.
2. Em caso de divergência entre os documentos referidos no número anterior, a prevalência é determinada pela ordem pela qual são indicados nesse número.
3. Em caso de divergência entre os documentos referidos no número 1 da presente cláusula e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o artigo 99.º do Código dos Contratos Públicos e aceites pelo Primeiro Outorgante nos termos do disposto no artigo 101.º do referido Código.

Cláusula 6.<sup>a</sup>

**(Preço)**

O preço global do contrato é de de 290.138,45€ (duzentos e noventa mil, cento e trinta e oito euros e quarenta e cinco cêntimos), ao qual acresce I.V.A. à taxa legal em vigor, de acordo com o seguinte escalonamento:

- 2025 – até 151.524,27€ (cento e cinquenta e um mil, quinhentos e vinte e quatro euros e vinte e sete cêntimos), incluindo o fornecimento de blocos adicionais, sem I.V.A.;
- 2026 – até 69.307,59€ (sessenta e nove mil, trezentos e sete euros e cinquenta e nove cêntimos), incluindo o fornecimento de blocos adicionais, sem I.V.A.;
- 2027 – até 69.306,59€ (sessenta e nove mil, trezentos e seis euros e cinquenta e nove cêntimos), incluindo o fornecimento de blocos adicionais, sem I.V.A..

Cláusula 7.<sup>a</sup>

**(Condições de pagamento)**

1. O Primeiro Outorgante obriga-se a pagar ao Segundo Outorgante o valor global constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, de acordo com o seguinte escalonamento:
  - 2025 – até 151.524,27€ (cento e cinquenta e um mil, quinhentos e vinte e quatro euros e vinte e sete cêntimos), incluindo o fornecimento de blocos adicionais, sem I.V.A.;
  - 2026 – até 69.307,59€ (sessenta e nove mil, trezentos e sete euros e cinquenta e nove cêntimos), incluindo o fornecimento de blocos adicionais, sem I.V.A.;
  - 2027 – até 69.306,59€ (sessenta e nove mil, trezentos e seis euros e cinquenta e nove cêntimos), incluindo o fornecimento de blocos adicionais, sem I.V.A..
2. O pagamento das facturas é efetuado no prazo de 30 (trinta) dias de calendário, a contar da data da sua receção pelo Primeiro Outorgante.
3. A forma e o processo de pagamento regem-se de acordo com as disposições legais que regulamentam a realização e o processamento de despesas da administração central

**Cláusula 8.<sup>a</sup>**  
**(Obrigações)**

- 1- O Segundo Outorgante obriga-se a executar o objecto do contrato de forma profissional e competente, utilizando os conhecimentos técnicos, o know-how, a diligência, o zelo e a pontualidade próprios das melhores práticas.
- 2- Constituem ainda obrigações do Segundo Outorgante:
  - a) Prestar os serviços e ou fornecer os bens conforme as condições de fornecimento definidas na sua proposta e demais documentos contratuais;
  - b) Assegurar os princípios da confidencialidade, integridade e disponibilidade da informação de acordo com as boas práticas de segurança de informação, preferencialmente em conformidade com a norma ISO/IEC 27002:2013, garantindo o alinhamento com a certificação ISO/IEC 27001 do IFAP, I.P.;
  - c) Assegurar que os recursos que afecta à prestação dos serviços objectos do contrato, detêm a formação académica ou a experiência profissional, a capacidade, o perfil e integridade profissionais adequadas ao desempenho das tarefas que lhes serão atribuídos, de forma correta, isenta e responsável;
  - d) Informar de qualquer facto que possa impossibilitar, total ou parcialmente, o cumprimento das obrigações contratuais decorrentes da celebração do contrato que possam comprometer a sua boa execução;
  - e) Não alterar as condições do fornecimento dos bens/da prestação dos serviços fora dos casos previstos nas especificações do presente contrato;
  - f) Recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação dos serviços, bem como ao estabelecimento dos sistemas de organização e informação necessários à perfeita e completa execução das tarefas a seu cargo, com a diligência e qualidade requeridas pelo tipo de trabalho em causa;
  - g) Não subcontratar, no todo ou em parte, a execução do objecto do contrato, sem prévia autorização do Primeiro Outorgante;

- h) Comunicar qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação social, os seus representantes legais, a sua situação jurídica e a sua situação comercial;
- i) Assegurar a receção do conhecimento descrito na Cláusula 10.<sup>a</sup> do presente contrato transmitido pelo Primeiro Outorgante ou por terceiro(s), pelo período mínimo de 1 (um) mês imediatamente anterior ao início da efetiva prestação dos serviços objeto do contrato;
- j) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenham no âmbito da formação e da execução do contrato, nem utilizar as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos;
- k) Observar as normas e procedimentos em vigor na entidade adjudicante no âmbito da segurança dos sistemas de informação (ISO27001:2013), em especial no âmbito da implementação de boas práticas, metodologia e segurança no desenvolvimento, nos acessos à informação e na gestão da mudança, os quais estão disponíveis para consulta;
- l) Nas situações aplicáveis, a solução a implementar tem de obrigatoriamente cumprir a Lei 36/2011 consubstanciada no RNID - REGULAMENTO NACIONAL DE INTEROPERABILIDADE DIGITAL.”
- m) Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato.
- n) Assegurar a inexistência de situações de incompatibilidade ou de conflito de interesses;
- o) Cumprir, na qualidade de subcontratante na aceção e para efeitos do disposto no n.º 8 do artigo 4.º do Regulamento (EU) n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril (o Regulamento Geral de Proteção de Dados, ou RGPD), as regras relativas à proteção das pessoas singulares nos termos do seu artigo 3º do ditado Regulamento e de acordo com as condições definidas no Anexo II ao presente contrato do qual faz parte integrante;

3. Excluem-se do âmbito do número anterior toda a informação gerada por força da execução do contrato, bem como todos os assuntos ou conteúdo de documentos que por força de disposição legal tenham de ser publicitados e/ou sejam do conhecimento público.

Cláusula 9.<sup>a</sup>

**(Dever de sigilo)**

- a) O Segundo Outorgante deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao Primeiro Outorgante, a que venha a ter acesso por qualquer meio, direta ou indiretamente, ao abrigo, ou relação com, a execução do contrato.
- b) Cabe ao Segundo Outorgante assegurar que os seus trabalhadores e colaboradores, independentemente do vínculo que com ele possuam, guardem o dever de sigilo na extensão prevista no número anterior.
- c) A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, incluindo a empresa com quem o Segundo Outorgante esteja em relação de grupo, nem ser objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do respetivo contrato.
- d) Excluem-se do dever de sigilo previsto nos números anteriores, a informação e a documentação que sejam comprovadamente do domínio público à data do seu conhecimento pelo Segundo Outorgante ou que este seja obrigado a revelar, por força da lei ou de ordem judicial recorível.”

Cláusula 10.<sup>a</sup>

**(Garantia de transferência e continuidade dos serviços)**

- a. A suspensão de determinado contrato ou a extinção do mesmo não prejudica a utilização plena pelo Primeiro Outorgante dos elementos produzidos no decurso da execução dos serviços e trabalhos e que são sua propriedade, nem a tomada de posse de todos os componentes relacionados, direta ou indiretamente, com o objeto do respetivo contrato.
- b. No caso previsto no número anterior, o Segundo Outorgante assume a obrigação de proceder à transferência, para o Primeiro Outorgante ou para terceiro(s) que a Primeiro Outorgante designar, de todas as informações relativas aos serviços, gestão e

operação e administração dos recursos tecnológicos que lhe foram confiados no âmbito do contrato celebrado, bem como a transferência da metodologias de todas as aplicações especificamente licenciadas e desenvolvidas para a entidade adjudicante e respetivos serviços de suporte tecnológico.

- c. O processo de transferência ou transição deve ocorrer no último mês de vigência do contrato, sob coordenação do Primeiro Outorgante, competindo ao mesmo a aceitação formal do processo de transferência tal como descrito no n.º 2 da presente cláusula.
- d. O Segundo outorgante compromete-se a executar os trabalhos de transferência em moldes que não prejudiquem a disponibilidade ininterrupta dos sistemas informáticos do Primeiro Outorgante, mantendo as responsabilidades e obrigações emergentes dos contratos, até estar finalizado o processo de transferência.
- e. Exceto nos casos de extinção do contrato por incumprimento do Primeiro Outorgante, todos os custos associados à execução dos trabalhos de transferência são da responsabilidade do Segundo Outorgante.

#### Cláusula 11.<sup>a</sup>

##### **(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. Entende-se por caso fortuito ou de força maior qualquer situação ou acontecimento imprevisível e excecional, independente da vontade das partes, e que não derive de falta ou negligência de qualquer delas.
- 3. 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 restabelecer a situação.

#### Cláusula 12.<sup>a</sup>

##### **(Alterações ao contrato)**

- 1. Qualquer alteração do contrato deverá constar de documento escrito assinado por ambos os outorgantes e produzirá efeitos a partir da data da respectiva assinatura.



2. A parte interessada na alteração deve comunicar, por escrito, à outra parte essa intenção, com uma antecedência mínima de 60 (sessenta) dias em relação à data em que pretende ver introduzida a alteração;
3. O contrato pode ser alterado por:
  - a) Acordo entre as partes, que não pode revestir forma menos solene que o contrato;
  - b) Decisão judicial ou arbitral;
  - c) Razões de interesse público.
4. A alteração do contrato não pode conduzir à modificação de aspectos essenciais do mesmo, nem constituir uma forma de impedir, restringir ou falsear a concorrência.

Cláusula 13.<sup>a</sup>

**(Resolução do contrato)**

1. Sem prejuízo de outras disposições legais e contratuais aplicáveis, considera-se existir incumprimento definitivo do contrato, o qual confere ao primeiro outorgante o direito de resolver o contrato, nos seguintes casos:
  - a) Insolvência, liquidação, cessação de atividade ou qualquer outra situação análoga resultante de um processo de idêntica natureza;
  - b) Incumprimento das suas obrigações relativamente aos pagamentos das contribuições para com a Administração Fiscal e Segurança Social nos termos das disposições legais aplicáveis;
  - c) Perda do registo de marca ou licença de comercialização;
  - d) Não comunicação de alterações à sua situação administrativa, jurídica ou comercial;
  - e) Falsas declarações;
2. O direito de resolução exerce-se mediante notificação, por carta registada com aviso de receção, dirigida ao segundo outorgante, da qual conste a indicação da situação de

incumprimento, no prazo de 30 (trinta) dias a contar do seu conhecimento pelo primeiro outorgante.

3. A resolução do contrato não prejudica o direito à indemnização que caiba ao primeiro outorgante nos termos gerais de direito.

Cláusula 14.<sup>a</sup>

**(Resolução por parte do contraente público)**

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, nomeadamente nos artigos 333.º a 335.º do CCP, o contrato pode ser resolvido nos casos a seguir indicados:
  - a) Incumprimento ou cumprimento defeituoso do contrato por facto imputável ao Segundo Outorgante;
  - b) Dissolução ou falência do Segundo Outorgante;
  - c) Incumprimento dos prazos determinados, por facto imputável ao Segundo Outorgante;
  - d) Cessão da posição contratual ou subcontratações não previamente mencionadas na sua proposta adjudicada, sem prévia aprovação escrita por parte do Primeiro Outorgante;
  - e) Incumprimento das políticas, práticas e procedimentos de segurança de informação da entidade adjudicante, incluindo as relativas às situações de incompatibilidade e de conflitos de interesse.
  - f) O contrato poderá ainda ser rescindido pelo Primeiro Outorgante ao fim de cada ano com aviso prévio de pelo menos 90 (noventa) dias.
2. O direito de resolução referido no número anterior exerce-se mediante comunicação escrita do Primeiro Outorgante ao Segundo Outorgante com indicação expressa dos respetivos fundamentos.
3. A resolução do contrato não prejudica a utilização plena pelo Primeiro Outorgante do que à data se encontrar implementado.

4. O disposto no presente artigo não prejudica a aplicação de quaisquer penalidades que se mostrem devidas, nem a reclamação de indemnização por danos.

Cláusula 15.<sup>a</sup>

**(Cessão da posição contratual)**

1. Não é permitida a cessão da posição contratual sem autorização prévia, por escrito, do Primeiro Outorgante.
2. A cessão da posição contratual obedece ao disposto nos artigos 317.º a 319.º do CCP

Cláusula 16.<sup>a</sup>

**(Subcontratação)**

1. Não é permitida a subcontratação sem autorização prévia, por escrito, do Primeiro Outorgante.
2. Em caso de subcontratação, o Segundo Outorgante mantém-se plenamente responsável pela prestação dos serviços objecto do contrato.

Cláusula 17.<sup>a</sup>

**(Sanções)**

- Em caso de incumprimento, pelo segundo outorgante, dos prazos previstos no contrato, por razões que lhe sejam imputáveis, poderá ser aplicada uma penalidade calculada de acordo com a fórmula:

$$P=Vx(A/1095)$$

Em que P corresponde ao montante de penalização, V é igual ao valor total do contrato e A é o n.º de dias em que se mantém o incumprimento ou cumprimento defeituoso do mesmo.

- O primeiro outorgante poderá deduzir no pagamento da factura que for devida, a importância correspondente às penalidades aplicadas, sem mais formalidades, nos termos do n.º3 do artigo 329.º do CCP.
- Sem prejuízo do disposto no número anterior, o incumprimento de prazos pelo segundo outorgante, pode determinar, para além do pagamento imediato penalidade apuradas

em resultado da aplicação da fórmula indicada, a resolução do contrato, a perda da caução a favor do primeiro outorgante e ainda o eventual dever de o indemnizar nos termos gerais.

#### Cláusula 18

##### **(Resolução sancionatória por incumprimento contratual)**

1. O incumprimento contratual definitivo confere ao primeiro outorgante o direito à resolução do contrato, nos termos do CCP.
2. A resolução do contrato não prejudica a aplicação de quaisquer sanções pecuniárias, nos termos da cláusula anterior.

#### Cláusula 19.º

##### **(Caução)**

O segundo Outorgante prestou caução nos termos do n.º 1 do artigo 89.º do CCP, no valor de 5% do valor global do contrato.

#### Cláusula 20.ª

##### **(Foro competente)**

O Segundo Outorgante renuncia a foro e submete-se em tudo, o que respeitar à execução do presente contrato, ao disposto na legislação portuguesa aplicável.

#### Cláusula 21.ª

##### **(Prazos e regras de contagem )**

À contagem de prazos na fase de execução do contrato aplicam-se as seguintes regras:

- a) Os prazos começam a contar a partir do momento em que o primeiro otorgante comunica a ocorrência ao segundo outorgante;
- b) Os prazos são fixados em dias de calendário;
- c) Quando o último dia do prazo for um dia de descanso semanal, obrigatório ou complementar, feriado ou um dia em que os serviços do primeiro outorgante, por qualquer causa, se encontrem encerrados, passa para o primeiro dia útil subsequente.

Cláusula 22.<sup>a</sup>

**(Comunicações e notificações)**

1. Com exceção do disposto no n.º 2 da cláusula 8.<sup>a</sup> do presente contrato, as notificações podem ser efetuadas por um dos seguintes meios:
  - a) Por correio eletrónico com aviso de entrega;
  - b) Por telecópia (fax);
  - c) Por carta registada com aviso de receção.
2. Os actos administrativos inerentes à execução do contrato só produzem efeitos após notificação nos termos previstos na presente cláusula.

Cláusula 23.<sup>a</sup>

**(Boa-fé)**

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

Cláusula 24.<sup>a</sup>

**(Uso de sinais distintivos)**

Nenhuma das partes pode utilizar a denominação, marcas, nomes comerciais, logótipos e outros sinais distintivos do comércio que pertençam à outra sem o seu prévio consentimento escrito.

Cláusula 25.<sup>a</sup>

**(Classificação orçamental)**

O presente contrato tem cabimento nas rubricas do orçamento de funcionamento do IFAP, I.P..

Cláusula 26.<sup>a</sup>

**(Omissões)**

Em tudo o que o presente contrato for omissivo, observar-se-á o disposto no Código dos Contratos Públicos, e demais legislação aplicável.

Lisboa, 10 de Janeiro de 2025

**RUI MANUEL  
COSTA  
MARTINHO**

Assinado de forma  
digital por RUI MANUEL  
COSTA MARTINHO  
Dados: 2025.01.13  
13:07:29 Z

O Primeiro Outorgante

Assinado por: **MIGUEL ANGEL SIMÕES SANTIAGO**  
Num. de Identificação: [REDACTED]  
Data: 2025.01.13 11:07:42+00'00'



O Segundo Outorgante

**Anexo I**  
(Características Técnicas)

**CONDIÇÕES TÉCNICAS DOS BENS E SERVIÇOS A FORNECER**

**1. BENS E SERVIÇOS A FORNECER**

O IFAP, I.P. pretende substituir o cluster de firewall existente, na sua infraestrutura de segurança de perímetro, beneficiando das mais recentes tecnologias que o mercado oferece com vista a mitigar os riscos emergentes a interligação com a rede pública. Para o efeito o presente procedimento tem como âmbito a modernização da atual solução:

- a) 2 x Firewalls 1U;
- b) 4 x SFP+ SR (10G) por equipamento;
- c) Renovação do UC:0007997010 (Consola de gestão e Acesso VPN, sem a componente de Capsule Workspace and Docs);
- d) As componentes CPCES-CO-STANDARD e CPSB-NGTP-15600-1Y (constantes do UC: 0007997010) deverão ser mantidas até à substituição da solução atual pelos novos equipamentos;
- e) Renovação do UC:0008453113 (Proteção de Email e Endpoint);
- f) Para fazer face à implementação das ferramentas de e-mail associadas ao MS Office 365, poderá haver a necessidade solicitar um incremento das licenças de proteção das caixas de correio eletrónico (Blocos Adicionais) da componente Checkpoint, durante a vigência do contrato, respeitando os preços propostos para o efeito. Os Blocos Adicionais considerados estão descritos no Anexo I. O valor apenas será pago se os Blocos Adicionais considerados forem ativados, a pedido do IFAP, I.P.;
- g) Suporte de 36 (trinta e seis) meses;
- h) Serviços de implementação e migração da solução atual.

## 2. REQUISITOS TÉCNICOS DOS BENS A FORNECER

As firewalls, a fornecer devem funcionar como cluster de 2 (dois) nós, e serem geridas pela atual consola de gestão (Check Point) mantendo todas as funcionalidades existentes. A solução deve permitir a implementação de proteções avançadas ao nível da política de acesso, e integração com o diretório ativo para autenticação e construção de políticas de acesso.

Ao nível do software devem ser garantidas as seguintes funcionalidades: Firewall, Identity Awareness, IPsec VPN (site-to-site) e Acesso remoto (VPN Cliente), IPS, Application Control, Content Awareness, URL Filtering, Antivirus/ Anti-Bot e DNS Security.

### a) Características & desempenhos (mínimos) das gateway firewall:

- Mínimo de 12 x portas 10G (SFP+) e 4 SFP+SR;
- Mínimo de 6 x portas 10/100/1000Base-T RJ45 (cobre);
- Opção para porta LOM (Lights-Out-Management) independente;
- N° VLANs  $\geq 1024$ ;
- Throughput (pacotes UDP 1518 byte)  $\geq 400$  Gbps;
- Sessões Concorrentes  $\geq 6,5$  milhões (até 29 Milhões, com upgrades de memória);
- Novas ligações por segundo  $\geq 535.000$ ;
- VPN Throughput (AES-GCM 1452B)  $\geq 75$  Gbps;
- IPS Throughput  $\geq 70$  Gbps;
- NGFW Throughput  $\geq 57$  Gbps;
- Threat Protection Throughput  $\geq 16,5$  Gbps;



- Memória RAM de 64 GB, expansível a 128 GB;
  - Disco rígido interno  $\geq 2 \times 950$  GB em SSD ou NVMe;
  - Fontes de alimentação redundantes;
- b) Possibilidade de expansão das gateway firewall:
- Sistemas virtuais  $\geq 20$  mínimo;
  - Carta de rede com 4 portas a 10/25G ou 2 portas a 40/100G;
- c) Funcionalidades gerais
- Suporte de clustering em Activo-Activo e Activo-Passivo;
  - Suporte de clustering com mais de 2 membros num mesmo cluster;
  - Detecção em tempo real de protocolos dinâmicos (ex: FTP, SIP, H323, etc.);
  - Detecção/bloqueio de serviços como P2P e IM por aplicação (voz/vídeo/file share);
  - Agrupamento de regras;
  - NAT de aplicações em tempo real;
  - PAT;
  - NAT/PAT baseado em regras;
  - Autenticação de serviços;
  - Integração com Active Directory e com LDAP;
  - Base de dados local de utilizadores;
  - Autenticação de 2 fatores (p. ex. tokens físicos, soft tokens, SMS e email);

- Geração interna e entrega de One Time Password (OTP) para autenticação;
- Implementação de regras com data de expiração ou em intervalos de tempo;
- Regras com objetos baseados na geografia;
- Identificação automática de utilizadores no sistema de logs;
- Reputação de Clientes;
- Suporte a proxy de HTTP e HTTPS;
- Regras por utilizador ou grupo de utilizadores;
- Captive Portal para autenticar utilizadores que não pertencem à rede;
- Contas Guest com gestão independente;
- Identificação de dispositivos (incluindo Fabricante e SO);
- Regras baseadas em dispositivos ou grupos de dispositivos;
- Possibilidade de controlo de endpoints;
- Opção de criação de gateways virtuais na mesma plataforma;

d) Networking

- Suporte Múltiplos Links WAN - Redundância e Balanceamento de carga;
- Routing baseado em políticas;
- Rotas Estáticas;
- IPv6;
- 802.1q- VLAN Tagging;

- DHCP Relay e DHCP Server;
- Spanning-Tree (802.1d);
- Suporte 802.3.ad e LACP - Agregação de Links (Activo-Activo ou Activo-Passivo);
- Suporte de Dead Gateway Detection;
- Job Scheduler;
- Suporte TOS/DiffServ;
- Suporte para Virtual Switches e para Virtual Routers;
- Instalação em modo Router e modo Transparente;

e) Networking em IPv6

- Rotas estáticas;
- RIPv6;
- BGP4+;
- OSPFv3;
- DNS;
- Endereçamento de interfaces;
- IPv6 Tunnel sobre IPv4;
- IPv4 tunnel sobre IPv6;
- Packet e network sniffing;

- NAT;
- Troubleshooting específico IPv6;

f) Protocolos de Routing

- OSPFv2 and v3;
- BGP;
- RIP;
- IGMP v2 and v3;
- Static and Multicast routes;
- Policy-based routing;
- PIM SM;
- PIM SSM;
- PIM DM;

g) Acessos VPN

- Serviço integrado nativamente e interno nas gateways;
- Licenciamento de utilizadores ilimitados, no que se refere a acesso VPN Client to Site em simultâneo, apenas restringido pelas limitações do hardware instalado.;
- Suporte de IKEv1 e IKEv2;
- Suporte de criptografia para 3DES e AES-256 para IKE Phase I e II IKEv2;
- Suporte de pelo menos os seguintes grupos de Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit);

- IKE Phase2 - Encriptação de dados (DES, 3DES, AES-128, AES-192, AES-256 e NULL) e suporte de integridade dos dados (MD5, SHA1, SHA256, SHA384, SHA512 e NULL)
- VPNs Site to Site: Full Mesh (all to all) ou Star (Remote to center);
- Suporte de IKE com PKI e pre-shared Secret;
- Aprovisionamento automático de VPNs site-to-site;
- Gestão automática de túneis IPSec de backup;
- Suporte de routing dinâmico em VPN IPSec;
- Clientes VPN para Windows, MacOS e iOS, Android;
- Suporte OTP para VPN sem recurso outros fabricantes ou servidores adicionais;
- Aplicação de políticas e restrições de acesso por utilizador ou grupos de utilizadores;
- Single Sign On VPN;
- Administração a partir da consola central;

#### h) IPS

- O fabricante deve fornecer evidências da sua posição de liderança, ano após ano, no Quadrante Mágico do Gartner para:
  - Soluções de Prevenção de Intrusão;
  - Soluções de Firewall Enterprise;
- O IPS deve ser baseado nos seguintes mecanismos de deteção:
  - Assinaturas;

- Anomalias no protocolo;
- Controlo Aplicacional;
- Análise de comportamento;
- Os Módulos de IPS e firewall devem estar integrados na mesma plataforma.
- O administrador deve ter a possibilidade de configurar a inspeção para proteção apenas da rede interna.
- O IPS deve ter opções para criar perfis com base em assinaturas para proteção de Clientes ou servidores. Também deve ser possível criar um perfil para proteção de ambos.
- O IPS deve fornecer pelo menos dois perfis/políticas predefinidas que podem ser utilizados no deployment da solução.
- O IPS deve ter um mecanismo fail-open baseado em software, ajustável com base em limites do gateway, CPU ou utilização de memória.
- O IPS deve ter mecanismo automático para ativar ou gerir as novas assinaturas após atualizações.
- O IPS deve suportar exceções com base em origem, destino, protocolo, ou uma combinação dos três.
- O IPS deve permitir mudar para o modo de deteção, sem alterar parâmetros individuais, por forma a facilitar as ações de troubleshooting.
- O IPS deve possuir uma solução centralizada de correlação e relatório de eventos.
- O administrador deve poder ativar de forma automática novas proteções, com base em parâmetros configuráveis:
  - Impacto no desempenho;

- Grau de severidade da ameaça;
  - Nível de confiança;
  - Proteções do cliente;
  - Proteções do servidor;
- O IPS deve ser capaz de detetar e prevenir os seguintes tipos de ameaça:
  - Uso indevido de protocolo,
  - Comunicações de malware,
  - Tentativas de uso de protocolos de tunneling,
  - Tipos genéricos de ataque sem assinaturas predefinidas,
- Para cada proteção, a solução deve incluir o tipo de proteção (relativamente a servidor ou cliente)
  - Gravidade da ameaça,
  - Impacto no desempenho,
  - Nível de confiança,
  - Referência - (ie CVE),
- O IPS deve ser capaz de capturar de pacotes/evidências para proteções específicas.
- O IPS deve ser capaz de detetar e bloquear ataques nas layers de network e application layer, protegendo pelo menos os seguintes tipos de serviços:
  - Serviços de email;
  - DNS;

○ FTP;

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

i) Application Control e URL Filtering

- A solução deve reconhecer e controlar mais de 6000 aplicações conhecidas.
- A base de dados da solução deve conter mais de 200 milhões de URL's categorizados, abrangendo mais de 85% da Alexa's top 1M sites.
- A solução deve permitir criar uma regra de filtragem de conteúdos com várias categorias.



- A solução deve permitir filtrar conteúdos de URL's baseada em HTTPS sem efetuar inspeção de SSL.
- A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias.
- A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores.
- A solução, após 4 semanas de produção, deve ter em cache cerca de 99% das solicitações de categorização.
- A solução deve ter uma interface fácil de pesquisa de aplicações e URL's.
- A solução deve categorizar aplicações e URL's por fator de risco.
- A política de URLF e Application Control deve poder ser definida por identidade do utilizador.
- A base de dados de URLF e Application Control devem ser atualizados por um serviço Cloud.
- A solução deve ter o controlo de aplicações e URLF unificado na mesma política.
- A solução deve ter mecanismos para informar ou perguntar ao utilizador em tempo real, para os educar ou para confirmarem as suas ações com base na política de segurança.
- A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda.
- A solução deve permitir exceções com base em objetos de rede previamente definidos.
- A solução deve fornecer a opção de modificar a página de Bloqueio e redirecionar o utilizador para uma página de remediação.

- A solução deve incluir um mecanismo de Black e White List, para permitir que se negue ou permita URL's específicos, independentemente da categoria.
- A solução deve fornecer um mecanismo de substituição na categorização de URL.

j) Anti-Bot e Anti-Vírus

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

- A solução de Anti-Bot e Anti-Virus deve ter um mecanismo centralizado de correlação e relatório de eventos.
- A solução de antivírus deve ser capaz de impedir o acesso a sites maliciosos.
- A solução de antivírus deve poder inspecionar o tráfego SSL.
- O Anti-Bot e o Anti-Virus devem ter atualizações em tempo real na cloud.
- O Antivírus deve ser capaz de impedir a entrada de arquivos maliciosos.
- O Antivírus deve ser capaz de analisar ficheiros compactados.
- Políticas antivírus e Anti-Bot devem ser geridas centralmente e ser possível a parametrização das mesmas.
- O Antivírus deve suportar a análise de links dentro de emails.
- O antivírus deve analisar ficheiros nos protocolos CIFS, SMBv3, HTTP, HTTPS, FTP, SCP e SFTP.

k) Condições de operação e alimentação

- Os equipamentos deverão funcionar em condições ambientais habituais em escritório, operando com temperaturas (°C)  $\geq 0$  e  $\leq 40$ , humidade (%)  $\geq 5$  e  $\leq 95$ , e serem energeticamente eficientes, possuindo pelo menos as certificações de segurança UL, CB, CE e TUV GS; de emissões FCC, CE, VCCI e RCM/C-Tick e ambientais RoHS, WEEE, REACH e ISO14001.
- MTBF superior a 10 Anos;
- Consumo máximo de 380W.

3. SERVIÇOS DE MIGRAÇÃO

- A solução proposta deve contemplar todos os serviços necessários à implementação da solução em produção. Não obstante deve o fornecedor, no mínimo, contemplar as seguintes tarefas:

- Reunião de planeamento;
  - Instalação física dos equipamentos;
  - Testes de funcionamento (off-line);
  - Migração das configurações da solução de segurança atual (Check Point);
  - Colocar em produção (trabalho a efetuar fora de horas);
  - Documentação da solução.
- Considerando a solução alvo de alteração devem ser considerados, no mínimo 5 (cinco) dias de serviços sendo que 50% dos serviços tem de ser realizados fora do horário laboral.

#### 4. SUPORTE

- Qualquer problema que impossibilite o normal funcionamento do sistema do IFAP, IP conduzirá à respetiva comunicação pelo IFAP, no mais curto espaço de tempo, tendo em vista a resolução do problema existente, considerando os tempos máximos para intervenção:
  - 4 horas (quatro horas) para resposta a problemas críticos que se traduzam na paragem do SISTEMA DE SEGURANÇA, tanto a nível de hardware como de software;
  - 8 horas (oito horas) para resposta a problemas não urgentes (que não impliquem a paragem imediata da solução), tanto a nível de hardware como de software;
- O número de intervenções necessárias a levar a cabo durante a vigência do contrato, por motivos de necessidade de manutenção de hardware/software (as referidas no ponto anterior) é ilimitado, dependendo das necessidades que se verificarem;

- As intervenções cobrem todo o hardware indicado, garantindo uma alternativa caso a assistência se encontre descontinuada pelo fabricante;
- Realização de um Plano de Contingência. O Plano de Contingência terá como objetivo apresentar um cenário de funcionamento alternativo ao atual SISTEMA DE SEGURANÇA no caso de uma paragem alargada do mesmo: Este plano deverá ser realizado logo após à assinatura do contrato e poderá ser atualizado a pedido do IFAP, I.P.;
- A pedido do IFAP, I.P. serão realizadas ações preventivas, com o objetivo de detetar falhas de segurança decorrentes da configuração implementada, e cujo respetivo resultado terá de ser consubstanciado em relatório, estas ações deverão distar entre si um mínimo de 6 (seis) meses;
- O horário de comunicações será:
  - Em todos os dias úteis, entre as 08.00h e as 20.00h para os problemas não urgentes;
  - 24X7 para os problemas críticos;
- Ao longo da vigência do contrato, e sempre que solicitado pelo IFAP, deverá ser garantida a atualização dos Sistemas Operativos, subscrição de software e de todos os Patches. Todas estas instalações deverão ser planeadas e agendadas com o IFAP de acordo com a disponibilidade de tempo e recursos;
  - A instalação de hardware e software nos sistemas do IFAP será sempre executada sob a responsabilidade do adjudicatário.

## 5. CONDIÇÕES E MÉTRICAS DE AVALIAÇÃO DA EXECUÇÃO DO CONTRATO

- As métricas a ter em consideração para a avaliação da execução do contrato são as seguintes:
- Ativação do suporte/manutenção junto dos fabricantes para o período contratado;
- 100% dos pedidos não urgentes respondidos em 4 horas;

- 100% de pedidos críticos respondidos em 24 horas;
- Instalação da nova solução de segurança nos 6 meses subsequentes à assinatura do contrato.

**Anexo II**  
(Listagem de Equipamentos)



| P/N                                                                      | Qtd.  | Descrição                                                                                                                                                                    |
|--------------------------------------------------------------------------|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Suporte e manutenção CHECK POINT                                         |       |                                                                                                                                                                              |
|                                                                          |       | UC: 0007997010 - de 21Jun2024 até 20Jun2025                                                                                                                                  |
| CP-HAR-EC-ADV-EMAIL-REN-1Y                                               | 1 000 | Advanced Anti-Phishing, including URL inspection and file sandboxing and sanitization (CDR), for incoming and internal Office 365 a                                          |
|                                                                          |       | UC: 0008453113 - de 21Jun2024 até 20Jun2025                                                                                                                                  |
| CP-HAR-EP-ADVANCED-REN-1Y                                                | 700   | Advanced threat protection for Endpoint devices, includes Web Protection, forensics Access protection, Sandbox emulation and extraction                                      |
| CP-HAR-EP-BASIC-REN-1Y                                                   | 300   | Basic threat protection for Endpoint devices, includes Web Protection, forensics Access and Data protection                                                                  |
| CP-HAR-RA-REN-1Y                                                         | 50    | Harmony Secure Remote Access - service for one user for 1 year                                                                                                               |
|                                                                          |       |                                                                                                                                                                              |
| P/N                                                                      | Qtd.  | Descrição                                                                                                                                                                    |
| Blocos adicionais ( 100 utilizadores ) - Harmony Email and Collaboration |       |                                                                                                                                                                              |
| CP-HAR-EC-ADV-EMAIL-1Y                                                   | 100   | Advanced Protect Anti-Phishing, including URL inspection and file sandboxing and sanitization (CDR), for incoming and internal Office 365 and Google Suite emails for 1 year |
|                                                                          |       |                                                                                                                                                                              |

**Anexo III**  
(Tratamento de Dados Pessoais)

**Secção I**  
**Notas Prévias**

De acordo com o Regulamento (EU) N.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril (o Regulamento Geral de Proteção de Dados ou RGPD), entende-se por:

- Dados pessoais - toda a informação relativa a uma pessoa singular identificada ou identificável (titular dos dados). Inclui dados como nome, número de identificação, dados de localização ou outros elementos que permitam chegar à identificação dessa pessoa singular. Estes dados podem constar de qualquer suporte, seja ele físico, virtual, tecnológico, sonoro ou gráfico;
- Tratamento - uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;
- Responsável pelo tratamento - a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais;

Os destinatários das comunicações de dados poderão ainda simultaneamente assumir a categoria de:

- Terceiros - pessoa singular ou coletiva, autoridade pública, serviço ou organismo que, não sendo o titular dos dados, nem o responsável pelo tratamento, nem o subcontratante, nem as pessoas que tratam dados pessoais sob a autoridade direta do responsável pelo tratamento ou do subcontratante, esteja autorizada a tratar dados pessoais mediante uma base legal específica para o efeito).



- Subcontratante - pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento desses dados, para as finalidades e com os meios de tratamento por este definidos ou determinados pelo direito da União Europeia ou de um Estado-Membro.

A Política de Privacidade do IFAP poderá ser alterada, considerando-se que as alterações entram em vigor a partir da data da sua colocação no link: [www.ifap.pt/privacidade](http://www.ifap.pt/privacidade).

### **TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO DA PRESTAÇÃO DE SERVIÇOS OBJETO DO CONTRATO**

1. O objeto do tratamento de dados pessoais, no âmbito da prestação de serviços objeto do contrato, é limitado:
  - a) Ao estabelecido no objeto do presente contrato.
2. A duração do tratamento de dados pessoais, no âmbito da prestação de serviços objeto do contrato, é limitada:
  - a) Ao estabelecido na duração/vigência do presente contrato, a menos que a conservação dos dados seja exigida ao abrigo do direito da União Europeia ou Nacional.
3. As categorias de dados pessoais sujeitos a tratamento, no âmbito da prestação de serviços objeto do contrato, são limitadas às seguintes:
  - a) DCF - Dados de identificação civil e fiscal
  - b) DDC - Dados de domicílio e contacto
4. Os grupos de titulares dos dados pessoais sujeitos a tratamento, no âmbito da prestação de serviços objeto do contrato, são limitados aos seguintes:
  - a) Colaboradores internos;
  - b) Corpos gerentes/Representantes de entidades coletivas;

5. O tratamento dos dados pessoais identificados no n.º 3 está, no âmbito da prestação de serviços objeto do contrato, é limitado às seguintes finalidades (F):
- a) Manutenção de instrumentos de gestão e atividades (A) de tratamento:
  - a) Gerir os sistemas de informação
6. No âmbito da prestação de serviços, objeto do contrato, o adjudicatário fica sujeito às seguintes condições no tratamento de dados que efetuar:
- a) tratará os dados pessoais de acordo com as instruções escritas da entidade adjudicante conforme Norma de Procedimento Externa de 25/06/2020.
  - b) Trata dados pessoais e assegura que quem trata dados pessoais o faz apenas de acordo com as instruções escritas que lhe sejam comunicadas, incluindo a “Política de Privacidade” disponível no portal do IFAP, a norma de procedimentos externa ID-050 – ANEXO III que estabelece os “Procedimentos a observar pelas entidades subcontratantes no âmbito do tratamento de dados pessoais por conta do IFAP, I.P.” ou outros que lhes sejam disponibilizadas para consulta, para o efeito, pelo IFAP, I.P.;
- § Esta norma poderá ser consultada nas Instalações do IFAP
- c) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
  - d) Adota as medidas para garantir um nível de segurança adequado ao risco;
  - e) Presta apoio ao IFAP através de medidas técnicas e organizativas adequadas, de modo a permitir que o IFAP, enquanto responsável pelo tratamento, possa cumprir a sua obrigação de dar resposta aos pedidos dos titulares dos dados no exercício dos seus direitos previstos no capítulo III do RGPD, nomeadamente o direito de acesso, o direito à retificação ou o direito de portabilidade dos dados;

- f) Presta apoio ao IFAP no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º, tendo em conta a natureza do tratamento e a informação que lhe foi disponibilizada;
- g) Conserva os dados tratados nos termos e condições que lhe foram comunicadas pelo IFAP;
- h) Informa o IFAP sobre o encarregado da proteção de dados que designou e os respetivos contactos;
- i) Colabora na realização de auditorias ou outras investigações, conduzidas pelo IFAP, por outro auditor, inspetor, ou perito por este mandatado, pela autoridade de auditoria ou pela autoridade de controlo nacional, a Comissão Nacional de Proteção de Dados (CNPd);
- j) Disponibiliza à CNPD as informações de que esta autoridade necessite no exercício das suas funções, bem como o acesso a todas as suas instalações, incluindo os equipamentos e meios de tratamento de dados, em conformidade com o direito processual da União Europeia ou nacional;
- k) Cumpre as recomendações que lhe forem feitas pelo IFAP ou pela CNPD e, se for caso disso, da forma e no prazo para o efeito determinado.
- l) Conserva um registo escrito e em formato eletrónico com todas as categorias de tratamento realizadas em nome do IFAP do qual constará:
  - i. As categorias de tratamentos de dados pessoais efetuados;
  - ii. Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança adotadas nos termos do artigo 32.º do RGPD.
  - iii. Disponibiliza, a pedido, o registo referido na alínea anterior à CNPD.

- iv. Notifica o IFAP sem demora injustificada, após ter conhecimento de uma violação de dados pessoais.
  - v. Disponibiliza ao IFAP todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na presente cláusula.
7. No âmbito da execução do contrato, o Fornecedor/Subcontratante recorre a outros subcontratantes apenas mediante autorização específica e por escrito do IFAP, I.P. e no respeito pelas mesmas condições que lhe são exigidas e previstas no presente Anexo.
8. No âmbito da prestação de serviços, objecto do contrato, o adjudicatário assume o estatuto de responsável pelo tratamento dos dados pessoais, sempre que, directamente ou por intermédio de um subcontratante a que tenha recorrido nos termos do número anterior, efectuar tratamentos:
- a) para finalidades distintas das definidas pelo IFAP;
  - b) com recurso a meios de tratamento distintos dos definidos pelo IFAP;
  - c) contrário às instruções do IFAP, salvo se a tal for obrigado por força de legislação europeia ou nacional aplicável.