

CADERNO DE ENCARGOS

PROCESSO N.º 2325000161

**Subscrição de solução SASE (*Secure Access Service Edge*) para assegurar o
acesso remoto de forma segura e eficiente aos recursos da rede do
Ministério do Trabalho Solidariedade e Segurança Social**

CAPÍTULO I DISPOSIÇÕES GERAIS

ARTIGO 1.º OBJETO DO CONTRATO

O presente caderno de encargos compreende as cláusulas do contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto principal a **aquisição do serviço de subscrição pelo Contraente Público da solução SASE (*Secure Access Service Edge*), ou equivalente, na modalidade de SaaS (*Software as a Service*)**, conforme discriminado no artigo 20.º 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 suprimimentos 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 DO COCONTRATANTE

SUBSECÇÃO I DISPOSIÇÕES GERAIS

ARTIGO 3.º OBRIGAÇÕES PRINCIPAIS DO COCONTRATANTE

Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorre para o **Cocontratante** a obrigação de disponibilização dos serviços identificados no artigo 20.º.

ARTIGO 4.º

CONFORMIDADE E OPERACIONALIDADE DOS SERVIÇOS

1. O **Cocontratante** obriga-se a prestar os serviços, com as características, especificações e requisitos técnicos previstos no presente Caderno de Encargos.
2. Os serviços devem ser prestados em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.
3. O **Cocontratante** é responsável perante o **Contraente Público** por qualquer defeito ou discrepância nos serviços objeto do contrato que existam quando sejam disponibilizados.

ARTIGO 5.º

DISPONIBILIZAÇÃO DOS SERVIÇOS

1. O **Cocontratante** obriga-se a disponibilizar os serviços objeto do contrato, de forma eletrónica por acesso ao site correspondente, no prazo de 7 dias a contar da celebração do contrato ou, caso seja necessária a migração, o prazo de 14 dias a contar da celebração do contrato (incluindo a migração).
2. O **Cocontratante** obriga-se a disponibilizar, simultaneamente com o início da prestação dos serviços objeto do contrato, todos os documentos, em língua portuguesa, que sejam necessários para a boa e integral utilização ou funcionamento daqueles.
3. Caso existam, todas as despesas e custos com a prestação dos serviços objeto do contrato e respetivos documentos são da responsabilidade do **Cocontratante**.

ARTIGO 6.º

INSPEÇÃO E TESTES

1. Efetuada a disponibilização dos serviços objeto do contrato, o **Contraente Público**, por si ou através de terceiro por ele designado, procede, no prazo de 15 dias, à inspeção dos mesmos, com vista a verificar, respetivamente, se os mesmos correspondem às características, especificações e requisitos técnicos e operacionais definidos no presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por Lei.
2. A inspeção a que se refere o número anterior é efetuada através dos testes.
3. Durante a fase de realização de testes, o **Cocontratante** 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 serviços 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 informar, por escrito, o **Cocontratante**.
2. No caso previsto no número anterior, o **Cocontratante** 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 serviços e o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
3. Após a realização das reparações ou substituições necessárias pelo **Cocontratante**, no prazo respetivo, o **Contraente Público** procede à realização de novos testes de aceitação, nos termos do artigo anterior.

ARTIGO 8.º

ACEITAÇÃO DOS SERVIÇOS

Caso os testes a que se refere o artigo 6.º comprovem a total operacionalidade dos bens e serviços 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 de 15 dias a contar do final dos testes, um auto de aceitação, assinado pelos representantes do **Cocontratante** e do **Contraente Público**.

ARTIGO 9.º

GARANTIA

1. Nos termos do presente artigo e da Lei que disciplina os aspetos relativos à compra e venda de bens, conteúdos e serviços digitais e das garantias a ela relativas, o **Cocontratante** obriga-se, a contar da data da assinatura do auto de aceitação, a prestar a garantia 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. O **Cocontratante** obriga-se igualmente a disponibilizar as atualizações (*“updates”* e *“upgrades”* de versão) durante o período da subscrição, no prazo de 5 dias a contar da comercialização;
3. Os serviços no âmbito da garantia abrangem o suporte *“on line”* ou telefónico, necessário ao bom desempenho do software, ininterruptamente (24hx365dias), com tempo de resposta de 4 horas e

com tempo de resolução em prazo razoável fixado pelo **Contraente Público** tendo em conta o interesse público envolvido.

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

ARTIGO 12.º

ACESSO ÀS INSTALAÇÕES

1. O **Contraente Público** garantirá ao **Cocontratante** o acesso às suas instalações e às instalações da Administração Pública envolvidas, para a realização dos trabalhos necessários ao cumprimento do presente contrato, caso necessário.
2. A permanência do **Cocontratante** nas instalações do **Contraente Público**, que implique paragem do sistema de informação instalado, deverá ocorrer fora das horas normais de serviço, salvo em situações necessárias a obviar a anomalias verificadas ou outras devidamente justificadas.
3. O **Contraente Público** acordará com o **Cocontratante** as normas de identificação do seu pessoal e os procedimentos adequados para acesso, permanência e circulação nas instalações.
4. O **Cocontratante** obriga-se a cumprir e a fazer cumprir as normas de identificação do seu pessoal e os procedimentos adequados para acesso, permanência e circulação nas instalações, de acordo com as determinações do **Contraente Público**, bem como à boa guarda e tratamento zeloso dos cartões de identificação disponibilizados pelo Contraente Público, assim como dos equipamentos e instalações.

SUBSECÇÃO II
DEVER DE SIGILO E CONFIDENCIALIDADE

ARTIGO 13.º
SIGILO E SEGURANÇA DA INFORMAÇÃO

1. O **Cocontratante** 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 **Cocontratante** 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 **Cocontratante** obriga-se:
 - a) A respeitar a confidencialidade sobre todos os dados disponibilizados pela ou pelas entidades envolvidas no projeto, bem como pelas informações de carácter 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 **Cocontratante** garante que terceiros que utilize na execução dos serviços respeitam os deveres referidos.
6. No âmbito das obrigações referidas no número anterior, o **Cocontratante** 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 **Cocontratante** não se iniciarão antes da entrega das declarações de sigilo.

ARTIGO 14.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, tecnológicos, ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas públicas.

SECÇÃO II
OBRIGAÇÕES DO CONTRAENTE PÚBLICO

ARTIGO 16.º
PREÇO

1. Pela subscrição do objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a **Contraente Público** obriga-se a pagar à Empresa Prestadora o preço até ao máximo constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
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 utilização de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças).
3. O preço base global é de **448 000,00 EUR (quatrocentos e quarenta e oito mil euros)**, a que acresce o valor do IVA à taxa legal em vigor.

ARTIGO 17.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 deve ser feito em **12** prestações mensais iguais e sucessivas, sendo que a primeira vence 30 dias após a aceitação.
3. Em caso de discordância por parte do **Contraente Público**, quanto aos valores indicados nas faturas, deve este comunicar ao **Cocontratante** 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 dos números anteriores, as obrigações relacionadas com os serviços só se vencerão se tiverem sido aceites pelo **Contraente Público**.
5. Sob pena de devolução, a fatura deve ser explícita quanto ao objeto do contrato e incluir, ainda, o número do compromisso e do pedido a transmitir pelo **Contraente Público** aquando da celebração do contrato.
6. O atraso no pagamento do preço constitui o **Contraente Público** na obrigação de pagar juros à taxa legalmente devida.

CAPÍTULO III INCUMPRIMENTO

ARTIGO 18.º PENALIDADES CONTRATUAIS E RESOLUÇÃO

1. Nos casos de atraso no cumprimento das obrigações referidas no n.º 1 do artigo 5.º, no n.º 2 do artigo 7.º, no n.º 2 e no n.º 3 (tempo de resolução) do artigo 9.º, bem como na alínea d) do n.º 1.2 do Anexo III do presente Caderno de Encargos, por motivos imputáveis ao **Cocontratante** ou a terceiros que utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula $P = \text{Preço Contratual} \times A/365$, 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 no n.º 3 do artigo 9.º (tempo de resposta) e na alínea a) do n.º 1.1.2.2. do Anexo III do presente caderno de encargos, e pelo não funcionamento dos serviços, por motivos imputáveis ao **Cocontratante** ou a terceiros que esta utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula $P = \text{Preço Contratual} \times A/1000$, em que P corresponde ao montante da penalização, e A é o número de horas.
3. Sem prejuízo das penalidades, a retribuição dos serviços não será devida pelo período em que o SaaS não funcione, por motivos imputáveis ao **Cocontratante** ou a terceiros que utilize no cumprimento da obrigação e sem prejuízo das consequências dos níveis de desempenho do SaaS constantes do n.º 1.3. do **Anexo III**.
4. Considera-se incumprimento definitivo, designadamente, quando houver incumprimento grave ou reiterado das obrigações referidas no artigo 13.º do Caderno de Encargos.
5. 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 **Cocontratante** e as consequências do incumprimento.

ARTIGO 19.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 Cocontratante, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do Cocontratante 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 Cocontratante de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo Cocontratante de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do Cocontratante 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 Cocontratante não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros; e
 - h) Eventos relacionados com os conflitos na Ucrânia e Israel.
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 20.º**DESCRIÇÃO DO OBJETO DO CONTRATO**

1. O software a subscrever, pelo período máximo de 12 meses a contar da aceitação, mas com termo final impreterível a 30 de junho de 2026, é o seguinte:

Designação comercial do produto (ou equivalente)	Quantidade
Licenciamento de Solução SASE Palo Alto Prisma Access	6000

2. Os requisitos mínimos são os seguintes:

- Acesso remoto para 6000 utilizadores concorrentes com o modelo de *Zero Trust* com suporte para os seguintes sistemas operativos (Windows, Mac OSX e Linux);
- Integração com Azure Active Directory para autenticação dos utilizadores;
- Integração com a Solução Microsoft Authenticator para segundo fator de autenticação (MFA)
- Plataforma virtual de Gestão Centralizada;
- Data Lake para suporte a solução;
- 2 interligações aos Datacenters do II (*Service Connections*);
- Ponto de Presença (POP) em Portugal (para assegurar a menor latência possível no acesso aos serviços e soluções alojados nos Datacenters do II localizados em Portugal) com a possibilidade de ativar o serviço em pelo menos 5 POPs à escolha a nível mundial a selecionar pelo Contraente Público;
- Análise da Experiência do utilizador em termos de desempenho do acesso, rede local, equipamento, acesso internet e às aplicações utilizadas.
- Acesso através de browser seguro a aplicações Web
- Funcionalidades de Segurança adicionais integradas:
 - Prevenção de Ameaças (*Threat Prevention*)
 - Filtragem de URL's / Endereços (*URL Filtering*)
 - Análise de conteúdo de ficheiros nomeadamente executáveis (*Sandbox*)
 - Segurança de DNS (*DNS Security*)
 - Prevenção de perda de dados (Data loss prevention -DLP)

3. Caso seja necessário, as tarefas de migração para a solução equivalente são da responsabilidade da Empresa Prestadora.

4. Os requisitos detalhados são os seguintes:

i. Arquitetura:

1. Serviço cloud com gestão nativa na cloud

2. Serviço suportado em rede global com mais de 100 Points of Presence espalhados pelo mundo. A solução deve permitir utilizar infraestrutura em qualquer destas localizações.
3. A solução deve garantir SLAs de disponibilidade mensal (pelo menos 99.999%) e conectividade (de menos de 10 ms de latência em termos de processamento de segurança, com cálculo horário) para acessos às principais aplicações SaaS (com uma latência inferior a 35 ms para acesso a aplicações SaaS alojadas no espaço europeu com cálculo diário).
4. Arquitetura de gestão multi-tenant
5. A infraestrutura (data plane) não deverá ser partilhada entre diferentes tenants. Ou seja, cada organização deverá ter infraestrutura dedicada, garantindo assim que não poderá ser afetada por qualquer outra organização que utilize a mesma solução.
6. Toda a infraestrutura que for criada para a organização deve ter IPs públicos dedicados que não sejam utilizados por qualquer outro cliente da solução. Desta forma pretende-se que os IPs utilizados pela organização nunca possam ser colocados em blacklists devido a comportamentos incorretos de outros clientes.
7. A solução deve permitir escalar automaticamente os recursos de computação no caso de haver um aumento do número de utilizadores da solução.
8. A solução deve permitir aumentar exponencialmente o número de utilizadores conectados sem necessidade de qualquer configuração ou alteração manual por parte dos administradores. A equipa de IT tem apenas de garantir que existe o licenciamento adequado para o número de utilizadores pretendidos.
9. A solução deve permitir estabelecer sem qualquer custo adicional duas ligações entre esta infraestrutura e os data centers da organização.
10. Deve ser possível configurar routing entre este serviço e os data centers da organização através de routing estático e BGP.
11. Este serviço deverá funcionar como uma extensão da infraestrutura do cliente.
12. A solução deve disponibilizar um agente com suporte para os seguintes sistemas operativos: Windows 10 e posterior, macOS 10.11 e posterior, iOS 10 e posterior, Android 5 e posterior e Linux nomeadamente CentOS, RHEL e Ubuntu
13. Para além de utilizadores remotos, deve existir a possibilidade de conectar escritórios remotos a este serviço através da criação de túneis IPSEC sobre a internet. Desta forma deve ser possível inspecionar e controlar o tráfego de determinados escritórios para a internet e para a rede corporativa a partir deste serviço.

ii. Requisitos gerais:

1. Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud
2. Permitir a implementação de uma estratégia de Zero Trust Network Access.

3. A solução deve identificar se as máquinas têm instalado os softwares e patches necessários para ter acesso à infraestrutura da entidade. Deve ser possível validar os mais diversos parâmetros das máquinas incluindo registry keys ou certificados presentes. Esta informação poderá ser usada na criação de políticas, de forma a limitar os acessos às máquinas que não respeitem as regras de compliance da organização.
4. A solução deve suportar os seguintes métodos de autenticação: SAML, TACACS+, RADIUS, LDAP, certificados, Kerberos e MFA.
5. Deve ser possível integrar a solução com plataformas de SIEM
6. Suportar integração com Azure AD e AD on-prem para obter informação sobre os grupos dos utilizadores.
7. Deve ser possível criar políticas de acesso às diferentes aplicações, com base no tipo de utilizador e/ou grupo assim como no estado da máquina utilizada para aceder às aplicações.
8. Deve suportar SSO
9. Deve ser possível que os utilizadores remotos se autenticuem de forma transparente sem a necessidade de ter constantemente de introduzir o seu username e password.
10. Deve ser possível estabelecer uma VPN entre a solução e os clientes remotos antes de estes fazerem login no seu computador.
11. Quando as máquinas da entidade se encontrarem fora da rede corporativa, todo o tráfego deve ser automaticamente enviado e inspecionado através deste serviço sem a necessidade de qualquer passo adicional por parte do utilizador.
12. No caso dos utilizadores remotos, o serviço deve escalar de forma automática, ou seja, se o número de utilizadores ligados aumentar significativamente quando comparado com a sua utilização normal (ex: 1000 utilizadores ligados em vez de 100), o serviço deve garantir o scale-up da infraestrutura cloud.
13. Deve ser possível inspecionar e controlar todo o tráfego entre os utilizadores remotos e as aplicações existentes nos Data Centers da organização.
14. A solução deve permitir publicar aplicações internas através de um portal de forma a serem acedidas por outras entidades.
15. Deve ser possível integrar esta solução com um serviço de SD-WAN do próprio fabricante.

iii. Funcionalidades base de Segurança

1. Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança;
2. Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino;
3. Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas;
4. Capacidade de identificação de subfunções dentro de uma aplicação;

5. Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7;
6. Possibilidade de agrupar aplicações por categorias de forma a que as políticas de segurança sejam aplicadas por categorias de aplicações;
7. Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP;
8. Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP;
9. Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL;
10. Capacidade de descriptar tráfego cifrado;
11. Capacidade de criar regras de QoS para determinado tipo de tráfego;
12. Capacidade de forçar o uso de MFA para acesso a determinados recursos. Deve ser possível configurar políticas que forcem qualquer utilizador em determinada subnet, a utilizar MFA se tentar aceder a um recurso em determinado segmento de rede da organização;
13. Num cenário onde a solução tenha o módulo de IPS ativo e se pretenda ativar qualquer um dos seguintes módulos: AntiVírus, Antispyware, DNS security, File Blocking ou Sandboxing não deve existir qualquer impacto na performance;
14. Todos os módulos da solução (ex: IPS, Antivírus, Antispyware, Sandboxing, DNS Security...) e respetivas assinaturas devem ser proprietários do próprio fabricante e totalmente controlados por este.

iv. Funcionalidades de Segurança Obrigatórias

1. IDS/IPS

- a. Capacidade de inspecionar o tráfego dos utilizadores de forma a detetar e prevenir a exploração de vulnerabilidades existentes.
- b. A solução deve disponibilizar *out-of-the-box* perfis de *best-practises* do fabricante de forma a simplificar a adoção da tecnologia.
- c. Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas
- d. Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades

2. Antivirus & Anti-Malware:

- a. Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C;
- b. Capacidade de habilitar mecanismos de DNS sinkholing que permitam intercepar pedidos de resolução de nomes para domínios comprometidos com malware;
- c. Capacidade de definir políticas de antivírus, de forma a que qualquer ficheiro transferido seja inspecionado e no caso de ser maliciosos seja bloqueado;
- d. Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp;



- e. Possibilidade de enviar o ficheiro para serviços de inspeção adicionais de sandboxing na cloud que permitam analisar e bloquear ficheiros maliciosos;
 - f. Capacidade de identificar ficheiros não através das suas extensões mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros;
 - g. Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro.
 - h. Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança.
3. Filtragem de URL's / Endereços (*URL Filtering*)
- a. Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar
 - b. Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud
 - c. Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação)
 - d. Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web
 - e. A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet
 - f. Para além de fornecer proteção contra phishing, a solução deve ser capaz de identificar qualquer utilizador, que tente utilizar as suas credenciais corporativas num site externo à organização. Para além de identificar esta situação a solução tem que ser capaz de a prevenir.
 - g. Deve ser possível classificar sites em múltiplas categorias (ex: alto risco e notícias)
4. Segurança de DNS (*DNS Security*)
- a. A solução deve suportar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos
 - b. Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes.
 - c. A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling).
 - d. A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS.



- e. Este serviço deve permitir identificar quais as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente.
 - f. A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente.
 - g. Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas.
 - h. Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos
 - i. A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças.
5. Análise de conteúdo de ficheiros nomeadamente executáveis (*Sandboxing*)
- a. Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload);
 - b. Perante uma análise por parte do serviço de Sandboxing na cloud que categorize a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente);
 - c. O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios;
 - d. A tecnologia de Sandboxing tem que ser capaz de inspeccionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP;
 - e. A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução;
 - f. Os sistemas de análise de malware devem ser capazes de detectar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux;
 - g. Em termos de suporte de sistemas operativos Windows emulados deve suportar: Windows XP, Windows 7 e Windows 10;
 - h. Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS),
 - i. Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF);
 - j. Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado.
 - k. Capacidade de descriptar malware (unpacker) para utilização na análise estática e machine learning.

6. Prevenção de perda de dados (Data loss prevention -DLP)

- a. A plataforma terá que suportar um módulo completo de Data Loss Prevention
- b. Esta funcionalidade deve ser disponibilizada como um serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente como por exemplo: Financeiros, Legais, Saúde, informação pessoal, etc. A solução deverá também permitir controlar este tipo de documentos de forma evitar a sua exposição ou extravio.
- c. Este serviço deverá permitir proteger estes documentos das seguintes formas:
 - Prevenir o upload de ficheiros com informação confidencial e/ou sensível para aplicações web não permitidas pela organização
 - Monitorizar o upload de documentos para aplicações externas permitidas pela organização
- d. O serviço deve disponibilizar *out-of-the-box* mais de 300 padrões de dados ("*data patterns*") e deve também disponibilizar perfis que agrupam determinados padrões de forma a simplificar a criação de políticas. Por exemplo, deverá existir um perfil associado com o GDPR de forma a facilitar a monitorização de documentos que possam contêm informação pessoal de utilizadores.
- e. A solução deverá ser constantemente atualizada com novos padrões e perfis.
- f. De forma a melhorar o rácio de deteção e eliminar falsos positivos a solução deverá permitir especificar: proximity keywords, níveis de confiança e expressões regulares básicas ou "weighted".
- g. Este serviço deve poder ser consumido por diferentes plataformas do fabricante, nomeadamente, firewalls, serviço SASE(Secure Access Service Edge), CASB(Cloud Access Security Broker) e CSPM(Cloud Security Posture Management). Isto permitirá aplicar políticas de DLP transversais à organização

v. Análise da Experiência do utilizador

- a. A solução terá que possuir um módulo de análise da Experiência do Utilizador (*Digital Experience Management*) que torne possível obter visibilidade sobre a performance de cada aplicação do ponto de vista do utilizador final.
- b. Este módulo deverá estar nativamente integrado com o agente da solução, garantindo assim que não existe qualquer necessidade de instalar qualquer agente ou appliance adicional.
- c. Deve ser possível identificar eventos que degradem a experiência do utilizador final em cada segmento entre o utilizador e a aplicação
- d. A solução terá que permitir a monitorizar aplicações SaaS, IaaS ou on-premises
- e. A solução terá que permitir monitorizar o endpoint do utilizador. Como parte desta monitorização a solução deve recolher a seguinte informação: utilização do CPU, memória em uso, uso do disco, "disk queue length", nível da bateria e informação sobre o wi-fi, incluindo SSID utilização de TX e RX BSSID e canal.

- f. A solução terá que monitorizar o tráfego real entre o utilizador e qualquer aplicação acedida independentemente da sua localização.
- g. A solução terá que utilizar testes sintéticos para criar um baseline da qualidade da rede e recolher informação sobre latência, jitter e perda de pacotes para cada segmento entre o utilizador e as aplicações. Devem também ser utilizados testes sintéticos para recolher métricas sobre as transações HTTP/HTTPS incluindo: disponibilidade da aplicação, uptime, latência HTTP, DNS lookup, SSL connect, time-to-first-byte e informação sobre a velocidade da transferência de dados.
- h. A solução terá que efetuar testes sintéticos nos seguintes segmentos: Utilizador - Router local; utilizador - Gateway SASE; utilizador - App; Gateway SASE - App. Isto deverá permitir identificar com exatidão qualquer segmento impactado e identificar o responsável por esse impacto (máquina do utilizador, rede externa à organização, rede interna ou aplicação acedida).
- i. Esta ferramenta deverá poder ser utilizada pelas equipas de IT/ServiceDesk para ajudar no processo de troubleshooting de potenciais problemas de conectividade de utilizadores remotos a aplicações SaaS ou internas.
- j. Terá que suportar sistemas operativos cliente Windows e MacOS.
- k. Este módulo terá que estar licenciado para todos os utilizadores da solução e não por quantidade de testes efetuados.

vi. Enterprise Browser

A solução terá que possuir um módulo de Acesso através de browser seguro com as seguintes características:

- a. Capacidade de acesso a aplicações privadas e internet.
- b. O utilizador não necessita de privilégios de administração para a instalação
- c. Customização de extensões, mensagens para a organização, bookmarks, etc
- d. Políticas e visibilidade unificada com a plataforma SASE
- e. Suportado em Windows, MacOSX, Android e iOS.
- f. Deve estender políticas Zero Trust em todas as ações e aplicações Web publicas ou privadas
- g. Aplicar controlo de identidade, acessos privilegiados e inibir acesso à informação no browser (última troço/*last mile*)
- h. Aplicação de regras com base na postura do equipamento
- i. JIT (Just in Time) para acesso a recursos privados ou públicos
- j. Suporte a acessos SSH/RDP e aceleração de tráfego
- k. Visibilidade de todos os acessos e ações dos utilizadores, com gravação de ecrã com base em regras definidas.
- l. Integração com Azure Active Directory para autenticação dos utilizadores (com suporte Autenticação SAML)
- m. Controlos de segurança no último troço (*last-mile*) e Identidade por Aplicação:

- Marca de água
- Controlo de PrintScreens/partilha
- Controlo de câmara/Microfone
- Restrições a instâncias/*tenants* SaaS
- Gestor de passwords do browser /Password Manager
- Aprovação de acesso por administradores
- Controlo de impressão
- *Data Masking*
- Proteção de ficheiros (com encriptação)
- *Typing guard*
- Restrições de login
- *Device Isolation*
- *Keylogger protection*
- *Screen scrappers protection*
- *Network security isolation*
- Trust certificate store
- *ML, OCR, EDM, IDM*
- Anti-tampering
- Advanced threat protection
- Advanced malware protection

CAPÍTULO V DISPOSIÇÕES FINAIS

ARTIGO 21.º TRABALHADORES

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

ARTIGO 22.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 23.º

CESSÃO DE CRÉDITOS

A cessão de créditos, designadamente no âmbito de contrato de “*factoring*” carece de autorização do contraente público.

ARTIGO 24.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 25.º

CÓDIGO CONDUTA

O Cocontratante 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 26.º

TRATAMENTO DE DADOS

1. Em virtude do necessário tratamento de dados pessoais inerente ao objeto do presente contrato, as Partes acordam em celebrar um Acordo de Processamento de Dados Pessoais, o qual faz parte integrante do presente contrato e se junta para todos os devidos e legais efeitos com o **Anexo II**.
2. Os requisitos de processamento de dados são exigíveis, independentemente de os dados serem pessoais, estando sujeitos às obrigações mencionadas no **Anexo III** do presente Caderno de Encargos.

ARTIGO 27.º

LEGISLAÇÃO APLICÁVEL

1. São aplicáveis, em especial, ao presente contrato os Capítulos IV e V do Título I e Capítulo III e IV do Título II, da Parte III do Código dos Contratos Públicos.
2. Ao presente contrato é, ainda, aplicável o artigo 419.º - A do CCP.

ARTIGO 33.º**CAUÇÃO**

1. A caução prestada para bom e pontual cumprimento das obrigações decorrentes do contrato, nos termos do Programa do Procedimento, pode ser executada pelo **CONTRAENTE PÚBLICO**, sem necessidade de prévia decisão judicial ou arbitral, para satisfação de quaisquer créditos resultantes de mora, cumprimento defeituoso, incumprimento definitivo pelo prestador de serviços das obrigações contratuais ou legais, incluindo o pagamento de penalidades, ou para quaisquer outros efeitos especificamente previstos no contrato ou na Lei.
2. A resolução do contrato pelo **CONTRAENTE PÚBLICO** não impede a execução da caução, contanto que para isso haja motivo.

ARTIGO 28.º**AVALIAÇÃO DO FORNECEDOR/ENTIDADE PRESTADORA**

O presente contrato será avaliado segundo os critérios do Manual de Avaliação de Fornecedores do **Contraente Público**, que se encontra publicado em www.seg-social.pt (“A Segurança Social” -> “Organismos” -> “Instituto de Informática, I.P.” -> “Manual de Avaliação de Fornecedores”).

ANEXO I
COMPROMISSO DE CONFIDENCIALIDADE
NPD 2325000161
(minuta)

Entre:

EMPRESA e

xxxxxxxxxxx Trabalhador/Colaborador,

CONSIDERANDO QUE:

- a) A **EMPRESA** vai prestar serviços que podem implicar a necessidade de aceder a informação ou a recursos de processamento de informação sob responsabilidade do Instituto de Informática, I.P.;
- 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 desenvolvimento dos serviços;
- 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 (ano)

A Entidade Patronal (EMPRESA)

O Trabalhador/Colaborador

ANEXO II

Acordo de Processamento de Dados Pessoais - Subcontratação

Considerando que:

- A. A **EMPRESA PRESTADORA** procederá ao tratamento de dados pessoais, de acordo com as especificações definidas no Caderno de Encargos;
- B. O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril, publicado no JOUE de 04 de maio de 2016, que aprova o Regulamento Geral de Proteção de Dados (de ora em diante RGPD), impõe um conjunto de obrigações na relação entre Responsáveis pelo tratamento e Subcontratantes, no que respeita ao tratamento de dados pessoais;
- C. O **CONTRAENTE PÚBLICO**, que age na qualidade de Subcontratante, tem obrigação de celebrar um acordo de processamento de dados com os seus Subcontratantes, por forma a garantir o cumprimento das regras subjacentes à recolha e tratamento de Dados Pessoais, segurança e privacidade de Dados definidas pelos Responsáveis pelo tratamento, de acordo com as exigências do RGPD;
- D. Pelo presente Acordo, serão estabelecidas as obrigações e deveres de ambas as Partes, para garantia de cumprimento do disposto no Considerando anterior.

É reciprocamente aceite o presente Acordo que se regerá pelos Considerandos anteriores, pelas cláusulas seguintes e, no que for omissivo, pela legislação aplicável:

Cláusula Primeira

Objeto e Finalidades de Tratamento

- 1. As Partes obrigam-se a definir e implementar as medidas técnicas e organizativas necessárias e adequadas ao cumprimento do RGPD e respetiva legislação nacional de execução, tendo em consideração o propósito do estabelecimento da relação entre as Entidades, bem como as inerentes atividades de recolha e tratamento de dados pessoais.
- 2. O presente Acordo tem por objeto o tratamento de dados no **contrato de subscrição da solução SASE para assegurar o acesso remoto de forma segura e eficiente aos recursos da rede do Ministério do Trabalho Solidariedade e Segurança Social**.

Cláusula Segunda

Categorias de Dados Pessoais envolvidos

São objeto de tratamento, para efeitos do presente Acordo, os seguintes dados pessoais: endereço IP de origem do acesso remoto e informação de localização associada.

Cláusula Terceira

Responsáveis pelo tratamento e Subcontratantes

No âmbito do presente Acordo, são considerados responsáveis pelo tratamento os serviços e organismos constantes do Decreto-Lei n.º 167-C/2013, de 31 de dezembro e os equivalentes ISSA, IPRA e ISSM, IP-RAM, e como Subcontratantes, o **CONTRAENTE PÚBLICO** e a **EMPRESA PRESTADORA**.

Cláusula Quarta

Obrigações dos Subcontratantes

1. Constituem obrigações da **EMPRESA PRESTADORA** e dos Subcontratantes ulteriores:

- a) Não subcontratar quaisquer Entidades para a prossecução de atividades, das quais resultem tratamento de Dados Pessoais, salvo quando exista autorização prévia e por escrito dos Responsáveis pelo tratamento ou do **CONTRAENTE PÚBLICO**;
- b) Fornecer toda a informação que lhes for solicitada, quer pelos Responsáveis pelo tratamento, quer pela Autoridade de Controlo, relativamente aos tratamentos dos dados, cujas finalidades se encontram definidas na Cláusula Primeira;
- c) Adotar as políticas de segurança e privacidade definidas na Cláusula Quinta;
- d) Obter as certificações exigidas legalmente, sempre que tais certificações contribuam de forma significativa para garantir eficazmente a proteção de dados pessoais;
- e) Garantir, em conjunto com os Responsáveis pelo tratamento e o **CONTRAENTE PÚBLICO**, o exercício por partes dos titulares dos dados pessoais dos direitos de informação, acesso, retificação, apagamento, oposição e limitação;
- f) A **EMPRESA PRESTADORA** constitui-se ainda na obrigação de permitir que o **CONTRAENTE PÚBLICO** proceda a auditorias regulares, como forma de assegurar que a execução do objeto do contrato é efetuada de acordo com as instruções indicadas e as medidas de segurança e privacidade definidas por aquele, incluindo as destinadas à verificação do cumprimento da alínea b) do n.º 4 do artigo 13.º do Caderno de Encargos;
- g) Assumir um compromisso de confidencialidade, quer com os trabalhadores que participem em operações de tratamento de dados pessoais, quer com colaboradores de entidades subcontratadas, desde que expressamente autorizadas pelo Responsável pelo tratamento;
- h) Não transferir os dados pessoais para um país fora da União Europeia ou para uma organização internacional, salvo quando exista autorização prévia e por escrito dos Responsáveis pelo tratamento ou do **CONTRAENTE PÚBLICO**;
- i) Inserir as obrigações sobre tratamento de dados, segurança e privacidade, previstas no contrato ou no acordo, nos contratos que celebrarem com subcontratantes ulteriores.

2. A **EMPRESA PRESTADORA** garante o cumprimento pelo subcontratante ulterior das obrigações por si contraídas neste acordo.

Cláusula Quinta

Medidas de Segurança e Privacidade

1. Para garantia de cumprimento do disposto no artigo 32.º do RGPD, deverão ser adotados padrões de segurança organizacional e tecnológica, com recurso a práticas eficazes na gestão de segurança da informação, para efeitos de proteção da confidencialidade, integridade e acesso àquela.
2. No âmbito do presente Acordo e para cumprimento do objeto do mesmo, deverão ser adotadas as medidas técnicas e organizacionais pertinentes para garantir um nível de segurança dos dados pessoais adequado ao risco, bem como contra destruição, perda, alteração, divulgação não autorizada, acesso accidental ou legal.
3. O previsto concretiza-se através da implementação das medidas definidas pelo standard internacional ISO/IEC 27001:20013, bem como das normas comunitárias, da legislação e das recomendações nacionais específicas em matéria de segurança da informação.
4. Nos termos e para os efeitos do disposto nos números 1 e 2, da presente Cláusula, deverão ser adotadas as medidas de segurança compatíveis com a Política de Segurança e Privacidade do **CONTRAENTE PÚBLICO**.

Cláusula Sexta

Confidencialidade

1. Para efeitos do presente Acordo, as Partes obrigam-se a não divulgar e/ou publicar qualquer informação a que tenham acesso, no âmbito da execução das suas atribuições.
2. A obrigação de confidencialidade prevista na presente cláusula, vincula as Partes durante a vigência do presente contrato e subsiste após a sua cessação, independentemente da causa da sua cessação.
3. A obrigação referida no n.º 1, cessa se a informação for do conhecimento público, exceto se tal acontecer em razão da violação do dever de confidencialidade imposto por esta cláusula.

Cláusula Sétima

Suspensão e/ou Resolução

1. A existência de fortes indícios de incumprimento do presente Acordo, de qualquer natureza, e/ou de incumprimento dos normativos constantes do RGPD e da legislação nacional de execução, é causa bastante para a suspensão do Contrato.
2. A efetiva existência de uma situação de incumprimento, quer do presente Acordo, quer dos normativos constantes do RGPD e da legislação nacional de execução, é causa bastante para a resolução do Contrato.

3. A verificação do disposto em qualquer dos números anteriores, tem como consequência direta a cessação da execução do objeto do presente Acordo.

Cláusula Oitava

Vigência

3. O presente Acordo de processamento de dados inicia os seus efeitos na data de assinatura do contrato que tem por objeto a aquisição, pelo Contraente Público, de **subscrição da solução SASE para assegurar o acesso remoto de forma segura e eficiente aos recursos da rede do Ministério do Trabalho Solidariedade e Segurança Social.**

ANEXO III

Requisitos de processamento de dados

1.1. Segurança

1.1.1. Requisitos de segurança geral:

O **Cocontratante** obriga-se ao seguinte:

- a) Proceder ao detalhe de “Logs” e eventos dos serviços adquiridos pelo **Contraente Público**;
- b) Proceder à encriptação dos dados, em repouso e em trânsito, entre os Centros de Dados;
- c) Adotar mecanismos de segurança pró-ativos, com recomendações de melhorias de segurança específicas, por serviço.
- d) Prestar os serviços a partir de dois centros de dados distintos situados na União Europeia em zonas que ofereçam proteção elevada quanto ao risco sísmico;
- e) Controlar as identidades e acessos mediante um sistema apropriado, com evidências a disponibilizar ao **Contraente Público** quando solicitado.

1.1.2. Requisitos de Cibersegurança:

1.1.2.1 O **Cocontratante** obriga-se a cumprir o Quadro Nacional de Referência para a Cibersegurança do Centro Nacional para a Cibersegurança de Portugal.

1.1.2.2. A ocorrência de incidentes de cibersegurança determina o cumprimento pelo **Cocontratante** das seguintes obrigações específicas:

- a) Notificar o **Contraente Público** no prazo de 1 hora a contar da deteção;
- b) Assim que possível, notificar o **Contraente Público** dos procedimentos destinados a mitigar e eliminar as consequências do incidente;
- c) Notificar, assim que possível, o **Contraente Público** da cessação do incidente, acompanhado do relatório com a informação relevante, designadamente, quanto aos danos provocados na informação deste

1.2. Informação

O **Cocontratante** obriga-se a disponibilizar ao **Contraente Público** o seguinte:

- a) Informação sobre cumprimento de standards relevantes do serviço;

- b) Relatórios de auditoria efetuados por entidades reconhecidamente independentes;
- c) Informação online do estado dos diferentes serviços SASE (disponibilidade e desempenho) e histórico de incidentes, com periodicidade mensal;
- d) Comunicação proactiva as falhas do serviço, no prazo de 1 dia, a contar da deteção

1.3. Nível de Serviço

- 1. Exige-se que a plataforma SASE possua um índice mínimo de disponibilidade de 99,999%;
- 2. Caso não se atinja mensalmente o índice mencionado no número anterior, ao valor a pagar, em cada prestação, serão deduzidos os montantes seguintes, independentemente da aplicação de penalidades:

Fórmula de cálculo:

Disponibilidade Mensal % = $(N.º \text{ Máximo de Minutos Disponibilidade} - \text{Indisponibilidade}) / (N.º \text{ Máximo de Minutos Disponibilidade} \times 100)$

<i>SLA atingido mensalmente</i>	<i>Desconto aplicado</i>
<=99,999%	5%
< 99.99%	10%
< 99.9%	15%
< 99%	25%
< 95%	100%

- 3. Com exceção do último mês de vigência do contrato, a dedução poderá ser substituída por crédito a imputar no mês seguinte.