



CADERNO DE ENCARGOS

PROCESSO N.º 2322000129

AQUISIÇÃO DE SERVIÇOS DE CONSULTORIA DE SEGURANÇA INFORMÁTICA NAS CAMADAS APLICACIONAL E DE BASE DE DADOS BASEADAS EM TECNOLOGIA ORACLE



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 pelo **Contraente Público** de serviços de consultoria de segurança informática nas camadas aplicacional e de base de dados baseadas em tecnologia Oracle.

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 suprimientos dos erros e das omissões do Caderno de Encargos identificados pelo concorrente, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c) O Caderno de Encargos;
 - d) A proposta adjudicada; e
 - e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

Capítulo II

Obrigações Contratuais

Secção I

Obrigações da Empresa Prestadora

SUBSECÇÃO I

Disposições Gerais

Artigo 3.º

Obrigações principais da Empresa Prestadora

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorre para a **Empresa Prestadora** a obrigatoriedade de prestar serviços de consultoria de segurança informática nas camadas aplicacional e de base de

dados baseadas em tecnologia Oracle, de acordo com as condições e requisitos do presente Caderno de Encargos.

2. A **Empresa Prestadora** fica ainda obrigada, a prestar os serviços afetando os recursos com os perfis, conforme exigido no nº 3.1. do **Anexo II** ao presente Caderno de Encargos.

Artigo 4.º

Forma de Prestação do serviço

Dada a natureza administrativa do contrato e a especial tecnicidade do respetivo âmbito, os serviços serão prestados em estreita articulação com a equipa interna do **Contraente Público**, de acordo com as regras referidas no presente documento e nos artigos 303.º a 305.º do Código dos Contratos Públicos.

Artigo 5.º

Vigência do contrato

O contrato produz efeitos na data de celebração e vigora por 12 meses.

Artigo 6.º

Propriedade Intelectual

1. Constituem propriedade originária do **Contraente Público**, todos os direitos intelectuais relativos aos módulos e outras criações previstas no presente contrato, incluído o direito de exploração exclusiva, assim como todos os elementos e afins (documentos, estudos, projetos, e material de conceção preliminar), desenvolvidos pela **Empresa Prestadora** ou pelos seus subcontratados, sem qualquer restrição, durante todo o prazo de proteção definido na Lei.
2. Os direitos acima referidos não abrangem os conhecimentos, experiência e *know-how* adquiridos durante a prestação de serviços objeto do presente contrato, pelo que a **Empresa Prestadora** poderá utilizar estes elementos para a prestação de serviços profissionais a terceiros.

Artigo 7.º

Exigência de Qualidade

1. A **Empresa Prestadora** 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. A **Empresa Prestadora** obriga-se a substituir qualquer recurso utilizado, a solicitação do **Contraente Público**, com fundamento na inadequação para o trabalho a desenvolver.

Artigo 8.º

Local de Prestação dos Serviços

Os serviços serão realizados na sede do **Contraente Público** ou no Centro de Processamento de Dados Principal em Loures, ou remotamente via acesso VPN, devidamente autorizada pelo **Contraente Público**.

Artigo 9.º

Acesso às Instalações

1. O **Contraente Público** garantirá à **Empresa Prestadora** o acesso às suas instalações e às instalações da Administração Pública envolvidas, para a realização dos trabalhos necessários ao cumprimento do presente contrato.
2. A permanência da **Empresa Prestadora** 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 as anomalias verificadas, ou outras devidamente justificadas.
3. O **Contraente Público** acordará com a **Empresa Prestadora** as normas de identificação do seu pessoal e os procedimentos adequados para acesso e circulação nas instalações.
4. A **Empresa Prestadora** obriga-se a cumprir e a fazer cumprir as normas de identificação do seu pessoal e os procedimentos adequados para acesso 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.

SUBSECÇÃO II

Dever de sigilo e confidencialidade

Artigo 10.º

Sigilo e Segurança da Informação

1. A **Empresa Prestadora** 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 a **Empresa Prestadora** 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, a **Empresa Prestadora** 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, a **Empresa Prestadora** garante que terceiros que utilize na execução dos serviços respeitem os deveres referidos.
6. No âmbito das obrigações referidas no número anterior, a **Empresa Prestadora** 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** ao presente Caderno de Encargos.
7. Os trabalhos e a utilização dos recursos pela **Empresa Prestadora** não se iniciarão antes da entrega das declarações de sigilo.

Artigo 11.º

Prazo do Dever de Sigilo

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

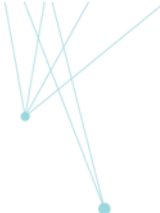
Secção II

Obrigações do Contraente Público

Artigo 12.º

Preço

1. Pela prestação dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o **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 deslocação 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 é de **250 000,00 EUR** (duzentos e cinquenta mil euros), acrescido do valor do IVA distribuído pelas seguintes parcelas:
 - a) Serviços proactivos: 150 000 EUR (cento e cinquenta mil euros), acrescido do valor do IVA;
 - b) Suporte reativo (nº 2.2 do Anexo II): 100 000 EUR (cem mil euros), acrescido do valor do IVA.



Artigo 13.º

Condições de Pagamento

1. A(s) quantia(s) devidas pelo **Contraente Público**, nos termos da cláusula anterior, deve(m) ser paga(s) no prazo de trinta dias após a receção da respetiva fatura, as quais só podem ser emitidas com o vencimento da obrigação respetiva;
2. O pagamento do preço será efetuado em 12 prestações mensais, iguais e sucessivas, depois da apresentação dos relatórios de atividades e documentos realizados no âmbito do serviço, o qual será comunicado ao **Contraente Público**, para validação prévia à emissão da respetiva fatura;
3. Em caso de discordância por parte do **Contraente Público**, quanto aos valores indicados nas faturas, deve este comunicar à **Empresa Prestadora** 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 só se vencerão se os serviços tiverem sido aceites e estiverem justificados pelo relatório de controlo de atividades e documentos relacionados com o serviço proativo a apresentar pela **Empresa Prestadora**.
5. Sob pena de devolução, a fatura deve identificar claramente o objeto do contrato, o esforço desenvolvido relacionado com a fatura, bem como, o número de pedido e de compromisso a transmitir pelo **Contraente Público** aquando da celebração do contrato.

Capítulo III

Incumprimento

Artigo 14.º

Resolução e Penalidades Contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, o **Contraente Público** pode exigir à **Empresa Prestadora** o pagamento de uma sanção pecuniária, nos seguintes termos:
 - a) Nos casos de atraso no cumprimento das obrigações previstas no n.º 2.2.1. do Anexo II e Anexo III (**Gravidade 1**) do presente caderno de encargos, por motivos imputáveis ao **Fornecedor** ou a terceiros que esta utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula $P = \text{Preço Contratual} \times A/200$, em que P corresponde ao montante da penalização, e A é o número de horas de atraso.
 - b) Nos casos de atraso no cumprimento das obrigações previstas no n.º 2.2.1. do Anexo II e Anexo III (**Gravidade 2**) do presente caderno de encargos, por motivos imputáveis ao **Fornecedor** ou a terceiros que esta utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula $P = \text{Preço Contratual} \times A/400$, em que P corresponde ao montante da penalização, e A é o número de horas de atraso.

- c) Nos casos de atraso no cumprimento das obrigações previstas no n.º 2.2.1. do Anexo II e Anexo III (**Gravidade 3**) do presente caderno de encargos, por motivos imputáveis ao **Fornecedor** ou a terceiros que esta utilize no cumprimento da obrigação, ser-lhe-á aplicada uma penalidade calculada de acordo com a fórmula $P = \text{Preço Contratual} \times A/600$, em que P corresponde ao montante da penalização, e A é o número de dias em atraso.
 - d) No caso de atraso no cumprimento das obrigações mencionadas no Anexo IV ser-lhe-á aplicada uma penalidade no montante 32 Euros por cada dia;
 - e) No caso de utilização de recursos em violação dos nºs 3.1. a 3.3. do Anexo II, ser-lhe-á aplicada uma penalidade no montante 100 Euros por cada hora por recurso envolvido;
- 2. Na determinação da gravidade do incumprimento, o **Contraente Público** tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do fornecedor e as consequências do incumprimento.
 - 3. O atraso no pagamento do preço constitui o **Contraente Público** na obrigação de pagar juros à taxa legalmente devida.

Artigo 15.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 da **Empresa Prestadora**, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades da **Empresa Prestadora** 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 pela **Empresa Prestadora** de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pela **Empresa Prestadora** de normas legais;
 - e) Incêndios ou inundações com origem nas instalações da **Empresa Prestadora** 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 da **Empresa Prestadora** não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros;
 - h) Eventos relacionados com a SARS-CoV-2; e
 - i) Eventos relacionados com o conflito na Ucrânia.
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 16.º

Requisitos e Condições da Prestação de Serviços

O enquadramento do serviço, bem como a descrição e respetivos requisitos de conteúdo técnico e funcional constam do **Anexo II** ao presente Caderno de Encargos.

Capítulo V

Disposições Finais

Artigo 17.º

Trabalhadores

A **Empresa Prestadora** obriga-se a cumprir com as obrigações decorrentes da legislação sobre trabalhadores estrangeiros, trabalho e segurança social.

Artigo 18.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 19º

Cessão de Créditos

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

Artigo 20.º

Seguros

1. Sem que isso constitua limitação das suas obrigações e responsabilidades, nos termos do contrato e deste Caderno de Encargos, a **Empresa Prestadora** deverá ser tomador de seguros que garantam o valor não só dos equipamentos como de eventuais danos que sejam causados pela indisponibilidade dos serviços objeto do presente procedimento.
2. A **Empresa Prestadora** deverá, nomeadamente, ser tomador das seguintes apólices de seguros:
 - a) Responsabilidade civil profissional, com cobertura dos riscos decorrentes dos trabalhos;
 - b) Responsabilidade civil extracontratual, por danos causados a terceiros decorrentes da execução dos serviços;
 - c) Seguro de acidentes de trabalho e doenças profissionais relativamente a todo o pessoal empregue na prestação dos serviços.
3. O **Contraente Público** poderá exigir a todo o momento ao Prestador de Serviços a apresentação das apólices de seguro e os recibos comprovativos do pagamento dos prémios respetivos.
4. Qualquer dedução efetuada pela Seguradora a título de franquia em caso de sinistro indemnizável será da conta da **Entidade Prestadora**.

Artigo 21.º

Foro Competente

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

Artigo 22.º

Legislação Aplicável

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

Artigo 23.º

Código de Conduta

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

Artigo 24.º

Processamento de dados pessoais

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, o qual faz parte integrante do presente contrato e se junta para todos os devidos e legais efeitos com o **Anexo V**.



ANEXO I

Compromisso de confidencialidade

2322000129

(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 1ª

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 2ª

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 20XX.

A Entidade Patronal

O Trabalhador/Colaborador

ANEXO II

Requisitos técnicos e funcionais para Prestação dos Serviços de consultoria de segurança informática nas camadas aplicacional e de base de dados baseadas em tecnologia Oracle

1. Enquadramento

1.1. Características do Sistema de Informação

O Sistema de Informação da Segurança Social (SISS) é um sistema integrado que engloba, entre outros, a identificação de todos os beneficiários, o registo das remunerações declaradas à Segurança Social, o cálculo e pagamento das prestações imediatas com mais impacto na população portuguesa tais como subsídios de desemprego e doença, além das pensões de velhice e invalidez e que, de uma forma geral, suporta todas as atividades diárias dos serviços da Segurança Social.

O SISS Inclui plataformas de portais transacionais dirigidos sobretudo ao cidadão dos quais se destacam: a Plataforma Transacional da Segurança Social, Segurança Social Direta, GFCT, Portais Informativos e um Sistema de Interoperabilidade, isto é, de interfaces aplicacionais com entidades externas nomeadamente AT, SIBS, AMA, IEFP, ESPAP, IGFEJ, SPMS.

A disponibilidade e performance dos vários serviços que fazem parte do SISS tem impacto a nível social, político e económico, afetando mais de 15 mil utilizadores internos (nomeadamente do ISS e IGFSS) e potencialmente, toda a população portuguesa.

Este sistema é crítico para o desenvolvimento da atividade de toda a Segurança Social, sendo baseado numa plataforma tecnológica complexa e de elevada dimensão nas seguintes componentes:

- Na diversidade de tipos e funções de componentes que suportam o negócio da Segurança Social e a missão do Instituto de planear, conceber, executar e avaliar as iniciativas de informatização e atualização tecnológica do MTSSS: armazenamento, processamento, comunicações e segurança, bases de dados, servidores aplicacionais, aplicações, entre outros;
- Na volumetria de componentes: 1200 máquinas, das quais 200 servidores aplicacionais J2EE, 150 bases de dados/400 TB de dados, mais de 900 BDs em SqlServer, 862 switches, 544 routers, 20 970 telefones VoIP, 400 pontos de acesso Wi-Fi, entre muitos outros;
- Nas funções que têm de ser asseguradas: análise de requisitos, implementação, acreditação e entrega de aplicações, instalação, configuração, evolução e administração de infraestruturas, realização e restauro de cópias de segurança, supervisão de sistemas e gestão de incidentes,

operação de sistemas e controlo de execução de processos massivos de processamento de dados.

- Nos destinatários e utilizadores servidos por estes sistemas e afetados em caso de falha.
 - Nestes incluem-se: cidadãos e empresas que acedem diretamente a portais públicos (Segurança Social, Segurança Social Direta, Fundos de Compensação, Incentivo ao Emprego, ASIP, OCIP, LNES, etc.), mais de 15.000 funcionários da Segurança Social e de outros parceiros no uso das aplicações de negócio; colaboradores internos ao Instituto de informática na prossecução das suas funções.
 - Só o portal Segurança Social Direta teve, em dezembro de 2021, mais de 2 milhões visitas correspondendo a cerca 1 milhão de visitantes únicos entre cidadãos e empresas.
- Nos números e montantes do negócio: a Segurança Social gere um orçamento de cerca de 28 mil milhões de euros de despesa.
 - As aplicações de negócio suportadas na infraestrutura gerida pelo Instituto de Informática asseguraram num mês o processamento de:
 - Mais de 2 milhões de pensionistas e de prestações e benefícios (abono de família, desemprego, doença, RSI, etc.)
 - Cerca de 1,9 milhões beneficiários, estes números juntaram-se, no mesmo período, medidas de apoio excecionais COVID a mais de 3 milhões de cidadãos e mais de 170.000 entidades empregadoras.

1.2 Objetivo e importância dos serviços

O SISS tem uma arquitetura tecnológica cuja camada de dados reside numa Base de Dados do fabricante Oracle em versão Enterprise Edition e a camada aplicacional em Servidores Aplicacionais Glassfish e Weblogic do fabricante Oracle.

Torna-se imperioso, perante as exigências legais em vigor, a atualização constante das políticas de segurança para prevenir eventuais vulnerabilidades das Bases de Dados e Servidores Aplicacionais do SISS.

O fabricante Oracle disponibiliza um serviço de consultoria denominado “Advanced Customer Service (ACS)”, que assegura um acompanhamento e implementação personalizado e pró-ativo com as seguintes características gerais:

- Ponto único de contato do cliente para problemas de suporte e gestão de níveis de escalonamento relacionado com temas de segurança e outros;
- Tratamento de solicitação de serviço prioritário;
- Suporte reativo e diagnóstico de problemas com grande impacto nos serviços;

- Aconselhamento preventivo fornecido com base em conhecimento específico do cliente;
- Aplicação de patches, configuração e proposta de melhoria dos produtos utilizados e de novas funcionalidades disponíveis bem como aconselhamento de arquiteturas Maximum Availability Architecture (MAA);
- Apoio na resolução de incidentes graves de segurança.

No caso concreto e tendo por enquadramento o cumprimento do RGPD e proteção do SISS, o fabricante Oracle disponibiliza um serviço que incide sobre o auxílio na implementação dos seguintes tópicos:

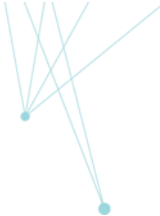
I. Segurança Lógica:

- Gestão de Acessos - Processos e controlos para assegurar Autenticação (forte) e autorização de utilizadores (ao detalhe), aplicações e serviços web; incluído cliente servidor, tecnologia web e móvel e prevenção de fraudes baseados em acesso ilícito;
- Gestão de Identidades - Processos e controlos para aprovisionar e desabilitar contas e privilégios nos sistemas, acessos e garantias de "privilegio mínimo", para segurança, auditoria e cumprimento, das políticas de acesso implementadas.

II. Segurança de Base de Dados:

- Controlo de Acesso a Base de Dados: Capacidade de assegurar acesso apenas a utilizadores autorizados e de controlo quem/onde/como os dados são acedidos;
- Monitorização e Auditoria: Capacidade de analisar ao nível da transação as atividades e monitorizar transações e informação histórica;
- Proteção de Dados: Processos e Métodos para segurança de dados de armazenamento, transmissão e acesso de dados da Organização durante o seu ciclo de vida;
- Configuração de Segurança: Processos e Métodos de segurança e cumprimento de políticas de segurança aplicados à configuração da Base de Dados;

Sem este serviço o Contraente Público aumenta fortemente o nível de risco associado à segurança da informação e poderá incorrer em penalidades segundo a mais recente normativa europeia RGPD. Adicionalmente é também uma componente fundamental para a certificação ISO 27001.



2. Caracterização dos serviços a prestar

2.1. O suporte proactivo:

- a) Definição da arquitetura de referência ao stack tecnológico Oracle aplicado ao Contraente Público;
- b) Atualização de componentes de software Oracle Advanced Security, Audit Vault e DataBase Vault para assegurar a sua evolução tecnológica e suportabilidade;
- c) Otimização de performance;
- d) Implementação de boas práticas Oracle, na exploração das plataformas de Base de Dados e respetivas ferramentas de segurança;
- e) Encriptação da Base de Dados, recorrendo designadamente às ferramentas Oracle Advanced Security, Audit Vault e DataBase Vault;
- f) Implementação de boas práticas Oracle, designadamente de segurança, na exploração das plataformas Weblogic e Glassfish;
- g) Possibilitar a prestação de serviços através da plataforma de Oracle Platinum Gateway;
- h) Suporte proativo/arquitetura:
 - h.1) Suporte às equipas do Contraente Público na operacionalização da estratégia e testes de segurança;
 - h.2) Acompanhamento e definição de roadmap para evolução destas componentes em conformidade com a RCM 41/2018.
- i) Suporte personalizado - assegurado por TAM (Technical Account Manager) dedicado:
 - i.1) Gestão de SRs (Service requests) e respetivo suporte;
 - i.2) Gestão de Serviço;
 - i.3) Priorização de SRs;
 - i.4) Ponto único de Contacto para questões relacionadas com o suporte de incidentes.

2.1.2. O serviço proactivo envolve a entrega dos documentos mencionados no Anexo IV

2.2. Suporte reativo:

- a) Acompanhamento às equipas de arquitetura, desenvolvimento e produção para esclarecimento de dúvidas e resolução de problemas relacionados com as tecnologias Oracle Advanced Security, Audit Vault e DataBase Vault;
- b) Revisão das configurações de Segurança e performance ao ambiente de produção;
- c) Análise de incidentes (Root Cause) e definição de planos corretivos;
- d) Revisão e suporte na aplicação de patches Oracle, em especial patches de segurança críticos;

- e) Apoio urgente na resolução a incidentes graves (Service Requests P1);
- f) Acompanhamento e suporte durante as passagens a produção;

2.2.1. O suporte reativo será prestado mediante os pedidos de intervenção e com os tempos de intervenção mencionados no Anexo III.

2.3. O serviço deve disponibilizar engenheiros, código, configurações, ferramentas, automações e procedimentos para as equipas internas do Contraente Público, que melhorem o nível de segurança da camada aplicacional e de base de dados, aumentem a capacidade de diagnóstico e resolução de problemas graves em exploração e proactivamente garantam a implementação de arquiteturas e configurações que assegurem uma máxima segurança, disponibilidade e performance dos sistemas.

3. Recursos

3.1. Perfil técnico dos recursos

Recursos adequados à prestação do serviço devem ter conhecimento da solução tecnológica instalada no Contraente Público no qual assunta o Sistema de Informação da Segurança Social, e que é suportada pelo software Oracle quer na componente Base de Dados quer na componente Aplicacional (Middleware).

Para este perfil os recursos devem ter as seguintes competências e experiência mínimas **obrigatórias** a comprovar pelo “curriculum vitae” e respetivas certificações em:

- a) Oracle Database 12c Administrator Certified Master ou superior;
- b) Oracle Database Administration 2019 Certified Professional OCP;
- c) Oracle Certified Expert, Oracle Database 12c: Data Guard Administrator;
- d) Exadata Certified Expert, Oracle Exadata X3 and X4 Administrator ou superior;

Experiência exigida:

- a) Experiência no mínimo de 8 anos nas funções de administrador em plataformas Oracle Database;
- b) Experiência no mínimo de 8 anos nas funções de administrador na plataforma Exadata;

3.2 Adicionalmente este perfil poderá ter as seguintes competências e experiência **opcionais** a comprovar pelo “curriculum vitae” e respetivas certificações em:

- a) Habilitações literárias ao nível da licenciatura no domínio da Informática ou similar;
- b) Oracle Database Cloud Administrator Certified Professional;
- c) Oracle Certified Expert, Oracle Database 12c: RAC and Grid Infrastructure Administrator;



3.3. Substituição de Recursos

- a) A mudança de recursos deverá ser autorizada pelo **Contraente Público**, nos termos do n.º 6 do artigo 75.º do CCP
- b) Sempre que qualquer recurso não possa comparecer, a **Empresa Prestadora** procederá à sua substituição por elemento previamente avaliado pelo **Contraente Público**;
- c) A substituição ou inclusão de novos recursos poderá ocorrer, por qualquer das partes, desde que devidamente justificada.
- d) Em caso de substituição de qualquer elemento da equipa, e sempre que necessário, será considerado um período de sobreposição de, no mínimo, 1 semana, sem custos para o **Contraente Público** para adaptação/formação do novo recurso.

ANEXO III

Níveis de Gravidade

1. Ao comunicar o pedido de intervenção, no âmbito do suporte reativo, o Contraente Público definirá a prioridade da intervenção nos seguintes termos:

- **Gravidade 1 (um)** - Indisponibilidade total dos serviços.

Resposta no prazo de 60 minutos a contar do pedido de intervenção;

- **Gravidade 2 (dois)** - Indisponibilidade parcial de várias componentes do serviço com impacto na performance.

Resposta no prazo de 90 minutos a contar do pedido de intervenção;

- **Gravidade 3 (três)** - Indisponibilidade de um conjunto reduzido de componentes, sem impacto na operação da solução e esclarecimentos técnicos e disponibilização de documentação.

Resposta no dia útil local seguinte a contar do pedido de intervenção.

2. O prazo razoável de resolução será fixado pelo Contraente Público tendo em conta a qualificação da Gravidade e o interesse público envolvido.



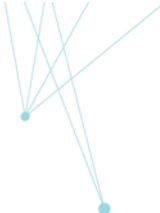
ANEXO IV

OBRIGAÇÕES DO SERVIÇO PROATIVO

- O apoio à instalação das atualizações dos componentes mencionados no nº 2.1. do Anexo II será prestado no prazo de 10 dias a contar da notificação do Contraente Público.
- Atividades específicas do serviço proativo:

Nº Serviços Proativos - Atividade	1º mês	2º mês	3º mês	4º mês	5º mês	6º mês	7º mês	8º mês	9º mês	10º mês	11º mês	12º mês
1 Definição da arquitetura de referência no stack tecnológico Oracle aplicado ao II												
2 Otimização de performance												
3 Implementação boas práticas Oracle, na exploração das plataformas de Base de Dados e respetivas ferramentas de segurança. Acompanhamento e definição de plano para evolução desta componente em conformidade com a RCM 41/2018;												
4 Revisão de cobertura de todas as vertentes de segurança aplicada a Base de Dados e recomendação eventual de novas soluções;												
5 Recomendações de segurança lógica no âmbito da Governância de Identidades e Gestão de Acessos;												
6 Atualização de componentes de software Oracle Advanced Security;												
7 Atualização de componentes de software Audit Vault e DataBase Vault para auditoria de segurança de Base de Dados;												
8 Encriptação da Base de Dados, recorrendo às ferramentas existentes no II, designadamente Oracle Advanced Security, Audit Vault e DataBase Vault;												
9 Avaliação de impacto de novas políticas de segurança no desempenho das Bases de Dados;												
10 Otimização de performance e revisão de política de Segurança por defeito;												
11 Suporte às equipas do II na operacionalização da estratégia e testes de segurança;												
12 Acompanhamento e definição de plano para evolução desta componente em conformidade com a RCM 41/2018												

- Cada uma das atividades envolve a entrega de um documento contendo as conclusões adequadas no prazo constante do número anterior.



ANEXO V

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 pelos seus Anexos 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 pessoais no âmbito do contrato de **serviços de consultoria de segurança informática nas camadas aplicacional e de base de dados baseadas em tecnologia Oracle**.

Cláusula Segunda

Categorias de Dados Pessoais envolvidos

- 1. São objeto de tratamento, para efeitos do presente contrato, os dados de identificação, incluindo nome e morada, bem como os pagamentos e recebimentos no âmbito do Sistema de Informação da Segurança Social.

2. Deve ser assegurada 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.

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 1.ª;
- 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 10.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 das obrigações por si contraídas neste acordo, caso exista subcontratação ulterior.

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 acidental 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 de **serviços de consultoria de segurança informática nas camadas aplicacional e de base de dados baseadas em tecnologia Oracle**.

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 presente Acordo.

Cláusula Oitava

Vigência

O presente acordo de processamento de dados inicia os seus efeitos com a celebração do **contrato de serviços de consultoria de segurança informática nas camadas aplicacional e de base de dados baseadas em tecnologia Oracle**.