



CADERNO DE ENCARGOS

(alínea b) do n.º 1 do artigo 40.º, conjugado com o artigo 42.º do Código dos Contratos Públicos)

PROCEDIMENTO AQUISITIVO N.º 107/ACT/DSI/2021

CONSULTA PRÉVIA

**CONTRATO MISTO DE AQUISIÇÃO DE 1.000 (MIL) LICENÇAS DE
SOLUÇÃO DE PROTEÇÃO E CONTROLO DA INFORMAÇÃO, COM
SUBSCRIÇÃO INICIAL DE 2 (DOIS) ANOS, *ONPREMISE*, BEM
COMO DOS SERVIÇOS DE IMPLEMENTAÇÃO E MANUTENÇÃO**

PARTE I CONDIÇÕES GERAIS

CAPITULO I DISPOSIÇÕES GERAIS

Cláusula 1.^a Apresentação

1. A Autoridade para as Condições do Trabalho, abreviadamente designada ACT, é um serviço integrado na administração direta do Estado, dotado de autonomia administrativa, com Sede na Avenida Casal Ribeiro, n.º 18-A, 1000 - 092, em Lisboa.
2. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do presente Procedimento de Consulta Prévia N.º 107/ACT/DSI/2021, sendo a Segunda Contratante a entidade com a qual será assinado o contrato em questão.

Cláusula 2.^a Objeto

O procedimento tem por objeto a celebração de um contrato misto de aquisição de **1.000 (mil) licenças de solução de proteção e controlo da informação, com subscrição inicial de 2 (dois) anos, onPremise, bem como dos serviços de implementação e manutenção**, de acordo com as Condições Gerais [Parte I] e as Especificações Técnicas [Parte II] constantes do presente Caderno de Encargos.

Cláusula 3.^a Contrato

1. O contrato será reduzido a escrito.
2. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
3. O contrato integra ainda, quando existam, os seguintes elementos:
 - a) O suprimento dos erros e das omissões, do Caderno de Encargos, identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;

- b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c) O Caderno de Encargos;
 - d) A proposta adjudicada;
 - e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
4. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.
5. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos (CCP) e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo Código.

Cláusula 4.ª

Prazos aplicáveis

1. **Prazo para Disponibilização da Solução:** a futura entidade adjudicatária deverá cumprir a obrigação de disponibilização da solução no prazo indicado em sede da proposta adjudicada, podendo este ser igual ou inferior ao limite temporal máximo estabelecido pela Divisão de Sistemas de Informação, de 30 (trinta) dias consecutivos, contados desde a data da assinatura do contrato.
2. **Prazo para Parametrização da Solução:** a futura entidade adjudicatária deverá concluir a parametrização da solução disponibilizada no prazo máximo de 60 (sessenta) dias consecutivos, contados desde a data da assinatura do contrato.
3. **Prazo para Entrada em Produção da Solução:** a entidade adjudicatária deverá a cumprir a obrigação de assegurar a entrada em produção da solução no prazo máximo de 60 (sessenta) dias consecutivos, contados desde a data da sua parametrização.
4. **Prazo Global de Execução do Contrato:** não obstante os prazos referidos nos n.ºs 1, 2 e 3 da presente cláusula, o prazo global de execução é de 2 (anos), contados desde a data de assinatura do contrato, uma vez que a

aquisição da solução inclui os serviços de manutenção da mesma, pelo período de 2 (dois) anos, para acesso a novas versões do *software*.

Cláusula 5.^a

Preço base

1. O **preço base** do presente procedimento é de **€ 70.325,00** (setenta mil, trezentos e vinte e cinco euros), acrescido de IVA à taxa legal de 23%, o que perfaz o **montante total de € 86.499,75** (oitenta e seis mil, quatrocentos e noventa e nove euros e setenta e cinco cêntimos).
2. Por forma a dar cumprimento aos n.ºs 2, 3 e 4 do artigo 35.º-A do CCP, informa-se dos termos e dos fundamentos da participação da «DIVULTEC - Serviços de Informática, Lda.» na preparação do presente procedimento de aquisição, cuja intervenção teve por objetivo auxiliar a ACT na definição e justificação do preço base tendo por referência critérios objetivos (cfr. n.º 3 do artigo 47.º do CCP), conforme descrito em sede da informação de suporte à abertura do procedimento.

CAPITULO II

OBRIGAÇÕES CONTRATUAIS

Secção I – Obrigações do Fornecedor

Subsecção I

Disposições Gerais

Cláusula 6.^a

Obrigações do fornecedor

A futura entidade adjudicatária deve:

- a) Apresentar proposta em resposta ao convite formulado pela ACT, no âmbito do presente Caderno de Encargos, com recurso à plataforma eletrónica acinGov;
- b) Fornecer a solução pretendida, bem como prestar os serviços de implementação e manutenção da mesma, em cumprimento dos prazos estabelecidos na cláusula 4.^a do presente Caderno de Encargos;
- c) Fornecer a solução pretendida e prestar os serviços de implementação conforme as condições definidas no presente Caderno de Encargos e demais documentos contratuais;

- d) Comunicar à ACT, logo que deles tenham conhecimento, os factos que tornem total ou parcialmente impossível o cumprimento de qualquer das suas obrigações, nos termos do presente Caderno de Encargos;
- e) Não alterar as condições do fornecimento dos bens e da prestação de serviços fora dos casos previstos no presente Caderno de Encargos;
- f) Prestar de forma correta e fidedigna as informações referentes às condições do fornecimento dos bens e da prestação de serviços, bem como prestar todos os esclarecimentos que se justifiquem;
- g) Comunicar à ACT qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação e sede social, os seus representantes legais, a sua situação jurídica ou a sua situação comercial;
- h) Comunicar à ACT a nomeação do Gestor do Contrato responsável e gestão do contrato celebrado, bem como quaisquer alterações relativamente à sua nomeação.

Cláusula 7.^a

Níveis de serviço, requisitos técnicos e funcionais

O fornecedor obriga-se a cumprir os níveis de serviço, requisitos e especificações constantes da Parte II do presente Caderno de Encargos.

Subsecção II

Dever de Sigilo

Cláusula 8.^a

Objeto do dever de sigilo

1. O fornecedor e todos os elementos da sua equipa de trabalho ou terceiros por si contratados devem guardar sigilo sobre toda a informação e documentação, técnica e não técnica, que venham a ter conhecimento em contacto com as atividades da ACT, ou que resultem da realização dos trabalhos, sob pena de conferir à ACT o direito de rescindir o contrato e ser indemnizada pelos danos causados.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, sem autorização prévia e expressa da ACT, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente a execução do contrato.

3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo fornecedor ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 9.ª

Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor indefinidamente, mesmo após a cessação do contrato, salvo declaração expressa em contrário pela ACT, 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.

Cláusula 10.ª

Direito de inspeção

1. A ACT reserva-se o direito de fazer inspecionar por delegados ou agentes seus, em todo e qualquer tempo ou lugar, ocasional ou permanentemente, a forma como o fornecedor executa o objeto do contrato, podendo rejeitar em todo ou em parte aquilo que for executado incorretamente, não esteja de acordo com as disposições contratuais ou com a boa prática profissional ou técnica corrente.
2. O exercício do direito de inspeção por parte da ACT não diminui, de qualquer modo, a responsabilidade do fornecedor no caso de posterior verificação de deficiente execução dos trabalhos contratados.

Cláusula 11.ª

Reuniões

Durante a execução do contrato poderão ser promovidas reuniões entre o fornecedor e a ACT ou entidades por esta designada.

Cláusula 12.ª

Marcas, patentes ou licenças

São da responsabilidade do fornecedor quaisquer encargos decorrentes de registo de marcas e patentes ou licenças, necessárias para a execução do contrato.

Secção II - Obrigações da ACT

Cláusula 13.^a

Preço contratual

1. Pelo fornecimento das 1.000 (mil) licenças e pela prestação dos inerentes serviços de implementação, formação e manutenção, que integram o objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a ACT pagará ao fornecedor o preço constante da proposta adjudicada, acrescido de cargas fiscais e parafiscais às taxas legais em vigor, se estas forem legalmente devidas.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à ACT, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 14.^a

Faturação e Pagamento

1. O preço indicado na proposta adjudicada será pago nos seguintes termos:
 - a) 50% do preço contratual após o cumprimento da obrigação de disponibilização das 1.000 (mil) licenças;
 - b) 50% do preço contratual com a entrada em produção da solução/aceitação do projeto.
2. As faturas só podem ser emitidas após o decurso da obrigação a que se reportam e serão pagas no prazo máximo de 60 (sessenta), dias após a sua receção pela ACT, através de transferência bancária para a conta do segundo outorgante.
3. O não pagamento total de uma fatura dentro do prazo referido no número anterior determina a constituição do primeiro outorgante em mora relativamente ao montante em dívida e a consequente obrigação de pagar juros moratórios correspondentes ao montante em causa, calculados à taxa legal, a partir do dia seguinte ao do vencimento da fatura até ao dia, inclusive, em que o pagamento integral desse montante seja efetuado na conta bancária do segundo outorgante.
4. Os juros moratórios devidos podem ser incluídos na fatura mensal seguinte de forma discriminada.

5. Em caso de discordância por parte da ACT, quanto ao valor indicado na fatura, deve esta comunicar ao fornecedor, por escrito, os respetivos fundamentos, ficando o fornecedor obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
6. Desde que devidamente emitida e observado o disposto no n.º 1, as faturas são pagas através de transferência bancária ou outro meio de pagamento acordado entre as partes.
7. A revisão de preços depende sempre de acordo entre as partes.
8. As faturas devem por um dos seguintes meios:
 - a) Para as instalações da Direção de Serviços de Apoio à Gestão (DSAG) da ACT, sitas na Praça de Alvalade, n.º 1, 1749 - 073, em Lisboa, ou
 - b) Para o endereço de correio eletrónico expediente.faturas@act.gov.pt, identificando, de forma inequívoca, a Referência do Procedimento Aquisitivo N.º 107/ACT/DSI/2021 e o objeto contratual.

Cláusula 15.ª
Gestor do Contrato

1. A ACT deverá designar um gestor do contrato, com a função de acompanhar permanentemente a execução deste, nos termos previstos pelo artigo 290.º-A do CCP.
2. A identificação do gestor do contrato constará do conteúdo do mesmo quando este for reduzido a escrito, conforme se prevê na alínea i) do n.º 1 do artigo 96.º do CCP.

CAPITULO III

PENALIDADES E RESCISÃO CONTRATUAL

Cláusula 16.^a

Penalidades contratuais

1. Pelo incumprimento dos prazos fixados para a disponibilização das licenças e para a prestação dos serviços, bem como das restantes obrigações constantes do presente Cadernos de Encargos, confere à ACT o direito a ser indemnizada através da aplicação de sanção pecuniária, nos termos dos números seguintes.
2. O valor da sanção pecuniária a aplicar é creditado a favor da entidade adquirente ou deduzido ao preço a pagar pelo fornecimento.
3. Em caso de incumprimento do disposto no prazo fixado para a realização da prestação de serviços, bem como das restantes obrigações constantes do Caderno de Encargos, por causa imputável ao adjudicatário, deverá ser aplicada uma sanção diária, de acordo com a seguinte fórmula:

$$P = V * A / \text{número total de dias de execução do contrato}$$

Sendo:

P = montante da sanção;

V = valor do contrato;

A = número de dias de atraso.

Cláusula 17.^a

Força maior

1. Não podem ser impostas penalidades ao fornecedor, nem é havida como incumprimento, a não realização pontual das prestações contratuais que 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 possa ser razoavelmente exigível contornar ou evitar.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

3. Não constituem força maior, designadamente:

- a) Circunstâncias que não constituam força maior para os subcontratados do fornecedor, na parte em que intervenham;
- b) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo fornecedor de deveres ou ónus que sobre ele recaiam;
- c) Manifestações populares devidas ao incumprimento pelo fornecedor de normas legais;
- d) Incêndios ou inundações com origem nas instalações do fornecedor cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
- e) Avarias nos sistemas informáticos ou mecânicos do fornecedor não devidas a sabotagem;
- f) Eventos que estejam ou devam estar cobertos por seguros.

4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.

5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 18.^a

Rescisão pelo fornecedor

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o fornecedor pode resolver o contrato quando qualquer montante que lhe seja devido pela ACT esteja em dívida há mais de seis meses ou o montante em dívida exceda 25% (vinte e cinco por cento) do preço contratual, excluindo juros.
2. Nos casos de dívida previstos no número anterior, o direito de resolução pode ser exercido mediante declaração enviada à ACT, que produz efeitos 30 (trinta) dias após a receção dessa declaração, salvo se este último cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.
3. Nos casos não abrangidos pelo número anterior, antes de proceder à rescisão, e se considerar que ainda é possível sanar o motivo de incumprimento, deverá a Segunda Contratante notificar a ACT da sua intenção, dos motivos porque pretende rescindir o contrato e fixar um prazo para que a ACT proceda à reparação das condições de incumprimento, findo o qual e se se mantiver esta situação, tornar-se-á efetiva a rescisão.

CAPÍTULO IV

MODIFICAÇÕES AO CONTRATO E SUBCONTRATAÇÃO

Cláusula 19.^a

Modificações objetivas do contrato

1. Durante o período de execução do contrato, a ACT poderá proceder a modificações objetivas do contrato nos termos previstos pelo artigo 311.º e seguintes do CCP.
2. Todas as modificações ao contrato, deverão constar de documento escrito subscrito e rubricado por ambas as partes.

Cláusula 20.^a

Subcontratação e cessão da posição contratual

A subcontratação pelo fornecedor e a cessão da posição contratual por qualquer das partes, depende da autorização da outra, nos termos do estabelecido no artigo 316.º e seguintes do CCP.

CAPÍTULO V DISPOSIÇÕES FINAIS

Cláusula 21.^a

Entrada em vigor

1. O contrato produz efeitos desde a data da sua assinatura até ao cumprimento de todas as obrigações previstas no mesmo e pelo período de 2 (dois) anos.
2. São encargos do fornecedor todas as despesas inerentes à celebração do contrato.

Cláusula 22.^a

Comunicações e notificações

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 CCP, para o domicílio ou sede contratual de cada uma, identificadas no contrato.

Cláusula 23.^a

Contagem de prazos

Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados, nos termos do artigo 471.º do CCP.

Cláusula 24.^a

Casos omissos

Em tudo o omissos no contrato observar-se-á o disposto no CCP e demais legislação aplicável.

Cláusula 25.^a

Foro competente

Para dirimir quaisquer questões ou litígios emergentes da interpretação ou violação do contrato, fica estipulada a competência do tribunal administrativo de círculo de Lisboa, com expressa renúncia a qualquer outro.

PARTE II – ESPECIFICAÇÕES TÉCNICAS

Enquadramento da Necessidade

1. A ACT procedeu, nos anos de 2015 e 2016, ao desenvolvimento de uma candidatura a fundos europeus com o objetivo de garantir comparticipação comunitária à implementação de um sistema de gestão da segurança da informação.
2. No âmbito do projeto SAMA SGSI - Sistema da Segurança da Informação, que se enquadrou essa candidatura, foi produzido um conjunto de documentação que visa constituir o Sistema de Gestão da Segurança de Informação da ACT.
3. As determinações constantes dos diferentes documentos, que compõem o SGSI estão em conformidade com as normas ISO/IEC 27001 (segurança da Informação), ISO/IEC 31000 (Gestão do Risco) e com algumas das exigências do Regulamento Geral de Proteção de Dados.
4. Este projeto constituiu uma contribuição ativa para a introdução de uma nova dinâmica na modernização administrativa ao nível da gestão e dos serviços – operacionalizando a desburocratização e a reengenharia de processos.
5. A atividade da ACT, desenvolvida por um grupo constituído por cerca de 950 (novecentos e cinquenta) funcionários, enquanto instituição de âmbito nacional e transversal no desempenho da sua missão definida pela tutela, assenta na atividade inspetiva e numa estrutura orgânica fortemente descentralizada, sendo condição conseguir obter ganhos de eficiência e de racionalização de recursos através da utilização intensiva e da integração dos sistemas de informação e de comunicação, realidade esta ainda distante.
6. Dada a importância que os meios eletrónicos e a maior apetência dos cidadãos e empresas para interações e relações mais céleres e menos

presenciais, é imperativo que também os serviços da administração pública sigam essa tendência e possam oferecer aos cidadãos os serviços de forma eletrónica, com o mínimo de fluxo de documentação em papel e de forma segura.

7. Dado o âmbito da documentação e informação que a ACT trata e gere, a segurança da informação adquire uma relevância significativa, especialmente quando se pretende disponibilizar serviços *on-line* e se solicita aos cidadãos e empresas a tramitação eletrónica de processos.
8. A Confidencialidade, Disponibilidade e Integridade da informação é crucial que seja garantida, para que se possam disponibilizar os serviços também na vertente eletrónica.
9. Com vista ao objetivo de disponibilizar serviços *on-line*, com recurso a métodos de autenticação eletrónica e se possa, de uma forma que garanta a segurança e confidencialidade de dados sensíveis, aderir à interoperabilidade da Administração Pública, tornou-se necessário desenvolver um modelo de Gestão do Risco e da Segurança da Informação.
10. Assim, o Sistema de Gestão de Segurança de Informação composto por cerca de 20 (vinte) documentos com instruções detalhadas sobre o tratamento das várias vertentes de informação e níveis de confidencialidade determinados e que está disponível na *intranet* organizacional para consulta pelos trabalhadores da ACT.
11. O contexto atual que vivemos, fomentou um aumento significativo da partilha de informação sensível através de sistemas de armazenamento na *Cloud*, a distribuição de informação sensível, através de ferramentas colaborativas e o acesso aos documentos via VPN, estes fatores implicam automaticamente um aumento do risco de dispersão e perda de informação.
12. Deste modo, a ACT necessita de uma solução que possibilite a proteção e controlo da informação, nomeadamente a informação confidencial, bem como a gestão de direitos de acesso, independentemente do local onde se encontrem os utilizadores, de forma a garantir a defesa contra a intrusão de acessos não autorizados e ciberataques à informação.
13. Para responder ao aumento do risco da segurança da informação, pretende-se adquirir uma solução que complemente a solução de

segurança de informação, recentemente adquirida, que seja eficaz na proteção da informação e gestão de direitos de acesso.

Cláusula 26.^a

Identificação geral da solução a adquirir

1. Face ao enquadramento exposto, o presente procedimento visa assegurar a aquisição e licenciamento de uma solução de cibersegurança nos termos previstos no presente caderno de encargos e que contemple os seguintes pontos:
 - a) Uma solução de proteção da informação e gestão dos direitos de acesso para garantir a defesa contra intrusão de acessos não autorizados e ciberataques à informação;
 - b) Serviços de implementação e manutenção.
2. A aquisição da solução inclui os **serviços de manutenção** da mesma, pelo **período de 2 (dois) anos**, para acesso a novas versões do *software*.
3. A solução deverá garantir:
 - a) Proteção da Informação:
 - i. Proteção da documentação dentro e forma da organização;
 - ii. Proteção de qualquer ficheiro *PDF*, *Office* e outros formatos de ficheiros com gestão de direitos digitais;
 - iii. Proteção automática de pastas em *SharePoint* e em Servidores de arquivos;
 - iv. Proteção para serviços de armazenamento em nuvem;
 - v. Proteção de pastas de *desktop*;
 - vi. Proteção de *e-mail*.
 - b) Permissões e Políticas de Controlo:
 - i. Permitir diferentes direitos de acesso, no que respeita às diversas ações a efetuar por cada utilizador ou grupo num determinado ficheiro (controlo total dos direitos de: ler,

editar, imprimir, copiar, gravar, etc.);

- ii. Permissões para grupos AD/LDAP;
- iii. Permissões para domínios e subdomínios;
- iv. Possibilidade e acesso *offline*;
- v. Possibilidade de acesso *offline* sem ter que abrir o documento anteriormente;
- vi. Possibilidade de definir datas de expiração do ficheiro;
- vii. Garantir que um utilizador que saiu da ACT, mesmo que na posse física de ficheiros da ACT não poderá aceder aos mesmos, em conformidade com as Políticas de Segurança.

c) Acesso a Informação Protegida:

- i. Acesso por utilizadores externos - utilizadores fora da organização podem aceder aos documentos onde tenham permissões;
- ii. Acesso a documentos do *Office* sem precisar de instalar *plugins* ou aplicações locais ou *web viewers*;
- iii. Suporte para aplicações *PDF* nativos e suporte para editar *PDFs*;
- iv. Abertura de mensagens protegidas sem precisar de um cliente de *e-mail* específico.

d) Cifrar um ficheiro e associar a permissão de acesso do mesmo a um indivíduo ou grupo;

e) Garantir que utilizadores específicos não possam retirar a cifra, por forma a assegurar que estes utilizadores ao partilharem o ficheiro indevidamente, o destinatário do seu envio não terá acesso ao mesmo;

f) Partilhar ficheiros cifrados com utilizadores externos e controlar o espaço temporal e com que permissões os mesmos podem aceder à informação;

- g) Aplicar a referida cifra a qualquer tipo de ficheiro suportado num *SO Windows*: incluindo CAD, TIFF, TXT, GIF, IMG, OFFICE, PDF, etc.;
- h) Ter relatórios de auditoria sobre as ações sobre os ficheiros nomeadamente quem fez o quê com determinado ficheiro, política ou permissão.
- i) A solução deverá, ainda, responder na integra aos requisitos técnicos para regular a contratação do serviço de proteção da informação e gestão de direitos de acesso, que se encontram especificados na cláusula seguinte e contemplar todos os utilizadores e unidades orgânicas da ACT.

Cláusula 27.^a

Especificações técnicas detalhadas da solução

1. A solução de proteção da informação e gestão dos direitos de acesso para garantir a defesa contra intrusão de acessos não autorizados e ciberataques à informação, deve garantir que a informação confidencial esteja sob controlo e protegida onde quer que esteja.
2. Nas alíneas seguintes encontram-se detalhados os **requisitos e especificações técnicas mínimas a cumprir pela solução**:

a) Proteção da Informação;

ID Req.	Requisito	Descrição	Tipo
Proteção da Informação			
REQPI01	Proteção da documentação dentro e fora da organização	A documentação está protegida e controlada dentro e fora da organização. É possível abrir documentos protegidos de fora da organização sem necessidade de VPN.	Obrigatório
REQPI02	Proteção de qualquer ficheiro PDF e Office com gestão de direitos digitais	PDF (Adobe, Foxit, Nitro), MS-Word, MS-Excel, MS-PowerPoint formatos suportados.	Obrigatório
REQPI03	Proteção de imagens com gestão de direitos digitais	Proteção com gestão de direitos de ficheiros digitais para jpg, jpeg, jpe, jfif, gif, bmp, dib, png, tif and tiff.	Obrigatório
REQPI04	Proteção de ficheiros AutoCAD com gestão de direitos digitais	Proteção com gestão de direitos de ficheiros digitais para AutoCAD v12 a versões atuais.	Obrigatório
REQPI05	Proteção de outros formatos de ficheiros com gestão de direitos digitais.	Proteção com gestão de direitos de ficheiros digitais para Simens JT e Solidworks.	Recomendado
REQPI06	Proteção de qualquer formato de ficheiro	Encriptação de qualquer formato de ficheiro com auditoria de acessos e possibilidade de revogação de acesso remoto.	Obrigatório
REQPI07	Proteção para serviços de armazenamento em nuvem	Proteção automática com a possibilidade de aplicar políticas por pastas, ficheiros guardados em Dropbox, OneDrive, Google Drive.	Obrigatório
REQPI08	Proteção de pastas de desktop	Proteção automática das pastas no desktop dos utilizadores	Obrigatório

REQPI09	Proteção automática de pastas em SharePoint	Proteção automática de pastas ou bibliotecas em SharePoint 2010, 2016 (On-premise, Online, Office 365).	Obrigatório
REQPI10	Proteção automática de pastas em Servidores de arquivos	Proteção automática com a possibilidade de aplicar políticas por pastas, ficheiros guardados em servidores de arquivos ou NAS.	Obrigatório
REQPI11	Proteção de e-mail	Proteção de ficheiros enviados por e-mail e do próprio texto do e-mail.	Obrigatório
REQPI12	Proteção sem fazer upload de ficheiros para a nuvem	Todos os processos de proteção devem ser executados localmente sem carregamento de nenhum ficheiro para a nuvem para proteção.	Obrigatório
REQPI013	Proteção com botão direito do Office ou simplesmente arrastando e soltando	Os utilizadores podem proteger documentos utilizando o menu contextual do Office, Outlook e até simplesmente guardar esses documentos em pasta sujeita à aplicação da política de proteção.	Obrigatório
REQPI014	Proteção em massa de documentos	A proteção em massa de documentos é possível através da seleção de várias pastas múltiplas, etc.	Recomendado

b) Permissões e políticas de controlo

ID Req.	Requisito	Descrição	Tipo
PERMISSÕES E POLÍTICAS DE CONTROLO			
REQCP01	Controlo das permissões de leitura, edição, impressão, cópia e colagem e controlo completo.	As políticas de proteção de ficheiros devem permitir selecionar quais dessas permissões são atribuídas à cada utilizador ou grupo de utilizadores.	Obrigatório
REQCP02	Permissões para grupos AD/LDAP	Possibilidade de conceder permissões a grupos Active Directory/LDAP.	Obrigatório
REQCP03	Permissões para domínios e subdomínios	Possibilidade de proteção para domínios e subdomínios completos (*@company.com , rh@*.company.com , *@* , etc.)	Obrigatório
REQCP04	Inclusão de marcas de água dinâmicas	Isto permite incluir água dinâmicas em documentos de forma que, quando o PDF é aberto, o utilizador vê o seu e-mail abrangendo cada página para reduzir a extração de capturas de ecrã.	Obrigatório
REQCP05	Possibilidade de “adicionar utilizadores”	Nas políticas de proteção, deve ser possível determinar quais utilizadores / grupos de utilizadores devem ter a capacidade de adicionar utilizadores à política sem a intervenção de um ficheiro protetor ou do TI.	Obrigatório
REQCP06	Possibilidade e acesso offline	É possível configurar o acesso offline por X dias a um documento protegido.	Obrigatório
REQCP07	Possibilidade de acesso offline sem ter que abrir o documento anteriormente	Para grandes volumes de arquivos, não é necessário abrir previamente cada documento online para poder abri-lo offline. Isso significa que o suporte de acesso offline é fornecido sem que o utilizador precise de abrir o documento anteriormente.	Obrigatório
REQCP08	Possibilidade de definir datas de expiração do ficheiro	Deve ser possível determinar datas a partir das quais o acesso não é permitido para os ficheiros protegidos. O sistema deve permitir a revisão desta data sem necessidade de voltar a proteger os ficheiros	Obrigatório
REQCP09	Criação de políticas de proteção pelos utilizadores	Isto permite que os utilizadores criem suas próprias políticas de proteção.	Obrigatório
REQCP10	Criação de políticas de proteção pelo administrador e atribuição para utilizadores ou grupos	Isto permite que o administrador crie políticas de proteção e as atribua a utilizadores específicos ou grupos de utilizadores de forma que eles estejam disponíveis para proteger os seus documentos.	Obrigatório

REQCP11	Possibilidade de ter gestores de ficheiros delegados	É possível designar “administradores de dados” internos que podem gerir as políticas de proteção para um grupo específico de utilizadores.	Obrigatório
REQCP12	Partilha de políticas pelos utilizadores	Um utilizador pode criar política de proteção e partilhá-la com outros utilizadores (ou grupos de utilizadores) na organização, desta forma eles podem utilizá-la para proteger documentos sem precisar de reconfigurar as permissões.	Obrigatório
REQCP13	Políticas particulares para utilizadores ou estudos de casos específicos	Os utilizadores só podem ver as políticas que o administrador criou para eles de maneira granular ou aquelas que eles próprios criaram. Isto significa que o Departamento Financeiro pode ver a política atribuída a este Departamento, mas não a do Departamento de Marketing.	Obrigatório
REQCP14	Acesso às informações das políticas pelos utilizadores e administradores	Os utilizadores protetor e administrador podem ver qual política foi atribuída a um documento específico. Os utilizadores que não têm Controlo Total podem ver apenas as permissões que possuem.	Obrigatório
REQCP15	Mudança de política de proteção	Os utilizadores e administradores podem modificar dinamicamente a política atribuída a um documento. No caso dos utilizadores, isso só pode ser feito se tiverem controle total na política de proteção.	Obrigatório
REQCP16	Controlo IP para política	O administrador pode configurar gamas de IP como requisito obrigatório para o acesso aos ficheiros protegidos com determinadas políticas, permitindo limitar a partir de onde a informação é acedida.	Obrigatório

c) Acesso à Informação Protegida

ID Req.	Requisito	Descrição	Tipo
Acesso à Informação Protegida			
REQAC01	Acesso por utilizadores externos	Utilizadores fora da organização podem aceder aos documentos onde tenham permissões	Obrigatório
REQAC02	Acesso à documentos do Office sem precisar de instalar plugins ou aplicações locais ou web viewers	O utilizador de documentos protegidos pode aceder um documento protegido do Office sem ter de instalar qualquer componente adicional para além do Microsoft Office; ou sem impor a utilização dum visualizador. A extensão dos ficheiros do Office não pode ser modificada após a proteção.	Obrigatório
REQAC03	Suporte para aplicações PDF nativos	Isto permite o acesso a documentos PDF protegidos utilizando Adobe Reader, Foxit Reader, NitroPDF, sem impor a utilização de visualizadores adicionais.	Obrigatório
REQAC04	Suporte para editar PDFs	Isto permite que documentos PDF protegidos sejam editados ou modificados se o utilizador tiver as permissões de editar ou modificar.	Obrigatório
REQAC05	Suporte ao cliente sem exigir privilégios de administrador	Para aceder documentos Adobe a partir do Microsoft Office, Adobe Reader, Foxit suites, etc. (sem utilizar visualizadores externos da Web), não é necessário instalar um agente que exija privilégios de administração.	Obrigatório
REQAC06	Abertura de mensagens protegidas sem precisar de um cliente de email específico	Para abrir mensagens protegidas, não é necessário instalar nenhum agente ou ser forçado a utilizar o Microsoft Outlook.	Obrigatório

d) Revogação e verificação de documentos

ID Req.	Requisito	Descrição	Tipo
Revogação e verificação de documentos			
REQREVO 1	Alteração acessos (administrador)	O administrador vai ter ferramentas para revogar ou rever os acesso a um documento ou grupo de documentos protegidos, mesmo que esses já tinham sido distribuídos.	Obrigatório
REQREVO 2	Alteração acessos (utilizador final)	O utilizador final vai ter ferramentas para revogar ou rever os acesso a um documento ou grupo de documentos protegidos por ele, mesmo que esses já tinham sido distribuídos.	Obrigatório
REQREVO 3	Transferência automática de propriedade de documentos	Deve ser possível transferir as permissões de propriedade ou acesso de um utilizador para outro, de um documento ou grupo de documentos protegidos, mesmo que eles já tinham sido distribuídos.	Obrigatório
REQREVO 4	Lista negra de utilizadores	É possível criar listas negras de utilizadores para bloquear (temporária ou permanentemente) o acesso a documentos protegidos.	Recomendado
REQREVO 5	Desproteção de documentos de emergência	No caso de uma emergência, o administrador deve ter a possibilidade de desproteger qualquer documento protegido	Obrigatório
REQREVO 6	Desproteção em massa de documentos	Se necessário, deve ser possível executar uma desproteção em massa de documentos e até mesmo colocar o sistema no modo de "desmantelamento" de tal forma que qualquer documento aberto seja automaticamente retirado.	Recomendado
REQREVO 7	Revogar utilizadores específicos ou grupos	A revogação permite remover o acesso de utilizadores ou grupos de utilizadores a documentos específicos	Recomendado
REQREVO 8	Desativando o acesso a documento para um utilizador qualquer	Deve ser possível bloquear o acesso a qualquer documento protegido para qualquer utilizador. Também deve ser possível desbloqueá-lo novamente, se necessário.	Recomendado

e) Monitorização e auditoria

ID Req.	Requisito	Descrição	Tipo
Monitorização e auditoria			
REQMON01	Alterar Acessos Permitidos pelo Administrador	O administrador terá ferramentas para alterar ou revogar o acesso a um documento ou grupos de documentos protegidos, mesmo que já tenham sido distribuídos.	Obrigatório
REQMON02	Alterar acessos permitidos para o utilizador final	O utilizador final pode alterar ou revogar revogar o acesso a um documento ou grupo de documentos protegidos por ele, mesmo que já tenham sido distribuídos.	Obrigatório
REQMON03	Auditoria de acessos a documentos protegidos pelo administrador	O administrador pode aceder relatórios ou tentativas de acesso não autorizados à documentos protegidos.	Obrigatório
REQMON04	Auditoria de acessos a documentos protegidos para os utilizadores finais	Os utilizadores com controlo total sobre um documento podem aceder relatórios ou tentativas de acesso não autorizado sobre o referido documento.	Obrigatório
REQMON05	Informação sobre ficheiros inacessíveis	Mesmo quando um arquivo não está fisicamente acessível, deve ser possível aceder todas as suas informações de auditoria (proteção aplicada, acessos, avisos, etc.).	Obrigatório
REQMON06	Relatórios Executivos	A plataforma deve apoiar o administrador na obtenção de relatórios executivos sobre o uso da plataforma; as proteções mais usadas, documentos mais partilhados com partes externas, utilizadores com mais tentativas de acesso não autorizado a documentos, documentos com mais avisos, etc.).	Obrigatório
REQMON07	Informações sobre documentos protegidos por utilizadores que não estão mais na empresa	O administrador pode obter informações sobre a política de proteção para um documento "inacessível" que os utilizadores não podem abrir.	Obrigatório
REQMON08	Auditar as ações executadas pelo administrador	As ações de modificação executadas nas políticas pelo administrador são salvas.	Obrigatório

f) Autenticação e gestão de identidade

ID Req.	Requisito	Descrição	Tipo
Autenticação e gestão de identidade			
REQAUT01	Integração com AD/LDAP	O sistema pode ser integrado no diretório ativo de tal forma que os utilizadores podem validar-se nele com as suas credenciais para o diretório ativo, então o seu registo ou eliminação do AD implica o seu registo ou eliminação do sistema; e a sua mudança do AD <i>group</i> implica a mudança automática nas suas permissões de documentação associadas a esses grupos.	Obrigatório
REQAUT02	Suporte para múltiplo domínios/ florestas de AD	Possibilidade de trabalhar com diferentes AD (Diretório Ativo) ao mesmo tempo. Suporte para ADs em diferentes florestas com e sem uma relação de confiança.	Obrigatório
REQAUT03	Automação e auto-registro de utilizadores externos	Deve ser possível automatizar o registo de utilizadores externos de tal forma que, quando eles são incluídos numa política, recebam automaticamente um convite para efetuar o seu próprio registo.	Obrigatório
REQAUT04	Personalização de convites e páginas de auto-registro	Os convites enviados por e-mail e ecrãs acedidos pelos utilizadores externos para o auto-registro podem ser personalizados com a imagem, logotipo e cores da empresa.	Recomendado
REQAUT05	Controlo de Auto-registo	O administrador pode controlar se os convites são enviados e quem pode enviá-los.	Obrigatório
REQAUT06	Utilizadores externos com contas de e-mail pessoais	Os utilizadores externos devem ter a possibilidade de usar contas de e-mail pessoais, por exemplo, Gmail.	Obrigatório
REQAUT07	Utilizadores externos no Active Directory ou base de dados local	Deve ser possível manter utilizadores externos num banco de dados interno, como no AD ou LDAP.	Obrigatório
REQAUT08	Possibilidade de criar diferentes organizações ou divisões no mesmo sistema	Cada organização pode ter administradores separados e extrair seus próprios relatórios. Todas as organizações devem poder trocar documentos entre elas (um único registo deve ser suficiente para todas elas). Todas as organizações podem estar num único AD / LDAP e com único administrador que pode gerir todas elas.	Obrigatório

REQAUT09	Dados em utilizadores internos e externos geridos localmente	Para uma solução instalada localmente, tudo, incluindo os utilizadores externos é mantido internamente e não há informações de que ela está incluída na nuvem do fornecedor.	Obrigatório
REQAUT10	Forçar reset de credenciais para utilizadores externos	Ao forçar o utilizador a alterar a senha, o administrador pode redefinir credenciais para os utilizadores externos que ele governa.	Obrigatório

g) Gestão e Administração

ID Req.	Requisito	Descrição	Tipo
Gestão e Administração			
REQADM01	Ferramenta de administração central baseada em web	A solução tem de administrada a partir de aplicação baseada em tecnologia web, sem requerer a instalação de aplicações ou plugins	Obrigatório
REQADM02	Gestão centralizada de políticas corporativas	O administrador pode gerir as políticas corporativas a partir de um painel central, atribuindo essas políticas aos utilizadores.	Obrigatório
REQADM03	Gestão central de políticas de utilizadores	O administrador tem acesso a políticas criadas pelos utilizadores para poder modificá-las, se necessário.	Obrigatório
REQADM04	Auditoria centralizada	Todos os acessos a documentos protegidos devem estar acessíveis de forma centralizada pelo administrador.	Obrigatório
REQADM05	Avisos sobre documentos	O administrador pode aceder os avisos sobre os documentos de maneira centralizada (documentos desprotegidos, tentativas de acesso bloqueado, etc.).	Obrigatório
REQADM06	Relatórios de resumo	O administrador tem acesso a relatórios de resumo sobre o uso das políticas específicas, os avisos sobre os documentos, os utilizadores mais ativos etc.	Obrigatório
REQADM07	Possibilidade de transferir permissões sobre documentos	O administrador pode transferir a propriedade dos documentos entre os utilizadores de tal forma que um utilizador perde o acesso a políticas específicas e outro utilizador o adquire.	Obrigatório
REQADM08	Modo de saída do superutilizador	O administrador pode verificar qualquer documento da organização, registando quais documentos foram retirados.	Obrigatório
REQADM09	Registo de utilizadores e grupos AD	O administrador pode registar utilizadores ou grupos de utilizadores AD/LDAP de forma automática	Obrigatório

REQADM10	Registro de utilizadores externos pelo administrador	O administrador pode registar utilizadores externos no painel de gestão e além disso podem ser convidados pelos utilizadores dentro da organização.	Obrigatório
----------	--	---	-------------

h) Implementação e integração

ID Req.	Requisito	Descrição	Tipo
IMPLEMENTAÇÃO/INTEGRAÇÃO			
REQDES01	Instalação com infraestrutura local	A instalação deve poder ser executada nas próprias infraestruturas do cliente.	Obrigatório
REQDES02	Instalação em máquinas físicas ou virtuais	A instalação deve poder ser executada tanto em máquinas físicas como virtuais (VMWare, Hyper-V).	Obrigatório
REQDES03	Alta disponibilidade	A instalação deve poder ser executada em alta disponibilidade (os dois: active-active e active-passive) e também <i>load balancing</i> .	Obrigatório
REQDES04	Integração com outras ferramentas	Deve ser possível integrar com ferramentas internas (plataformas internas do cliente) via SDK ou webservice	Obrigatório
REQDES05	Integração com DLPs	Deve ser possível integrar a solução com DLPs. Pelo menos, Symantec, McAfee ou ForcePoint.	Obrigatório
REQDES05	Integração com classificadores de informação	Deve ser possível integrar a solução com ferramentas de classificação como Boldon James, Titus, etc. e qualquer outra solução que funcione modificando os <i>metadados</i> dos ficheiros.	Obrigatório
REQDES06	Integração com soluções de gestão de eventos	A ferramenta deve possibilitar a exportação automática de eventos para soluções tipo SIEM	Obrigatório

i) Plataformas Suportadas

ID Req.	Requisito	Descrição	Tipo
PLATAFORMAS SUPORTADAS			
REQSP01	Suporte para a plataforma Windows Client.	Possibilidade de proteger documentos e aceder documentos protegidos nas versões Windows XP, Vista, 7, 8, 8.1 e 10.	Obrigatório
REQSP02	Suporte para a plataforma Windows Server.	Possibilidade de proteger documentos e aceder documentos protegidos no Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016.	Obrigatório
REQSP03	Acesso a partir do Mac OSX e plataformas móveis.	Possibilidade de visualizar documentos protegidos nas plataformas Mac OSX, iOS (iPad, iPhone) e Android.	Obrigatório
REQSP04	Office suites 2003, 2007, 2010, 2013, 2016, 2019, Office 365	Suporte para as versões do Microsoft Office de 2003 a 2019 e do Office 365.	Obrigatório
REQSP05	Adobe, Foxit, NitroPdf e Nuance suites.	Suporte para abrir documentos protegidos com o Adobe Reader, Foxit, NitroPDF, Nuance (PDF suites com DRM suporte).	Obrigatório

Cláusula 28.^a

Identificação dos serviços a adquirir

1. Para além da aquisição de 1.000 (mil) licenças de solução de proteção e controlo da informação, a ACT pretende adquirir igualmente os seguintes serviços de implementação e manutenção:
 - a) Gestão de projeto;
 - b) Desenho técnico da solução;
 - c) *Staging* e configuração em ambiente controlado. Devem ser instalados até 10 (dez) postos de trabalho em ambiente controlado e representativo da ACT;
 - d) Testes;
 - e) Preparação e planeamento da instalação 1.000 (mil) utilizadores:

- i. Preparação *template, script*, GPO;
 - ii. Instalação 1.000 (mil) utilizadores. A instalação do *software* nos postos de trabalho dos utilizadores é da responsabilidade da ACT
 - iii. Apoio à ACT na instalação (mínimo 2 dias);
- f) Formação (*On-Job*) equipa técnica da ACT, em datas a agendar oportunamente entre as partes;
 - g) Elaboração de guia prático (*quick guide*) para utilizadores;
 - h) Documentação de projeto.
2. Os serviços a realizar devem seguir as regras de boa prática na implementação de projetos semelhantes.
 3. A solução deverá incluir manutenção de *software* pelo período de 2 (dois) anos para acesso a novas versões de *software*.