AUTORIDADE PARA AS CONDIÇÕES DO TRABALHO

UNIÃO EUROPEIA
Fundos Europeus Estruturais e de Investimento

COMPETE 2020

Aprovado.
Nelson Ferreira
Assinado de forma digital por Nelson Ferreira
Dados: 2020.12.03 09:39:42 Z
Competências delegadas pelo Despacho n.º 11077/2020, publicado no Diário da República, 2.ª série, N.º 220, de 11 de novembro de 2020

CADERNO DE ENCARGOS

CONSULTA PRÉVIA

PROCEDIMENTO DE AQUISIÇÃO DE UMA SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO, A INSTALAR ON-PREM, CONSIDERANDO UMA SUBSCRIÇÃO INICIAL DE 1 ANO, A UM UNIVERSO DE 1.000 UTILIZADORES, INCLUINDO OS SERVIÇOS DE INSTALAÇÃO, IMPLEMENTAÇÃO, CUSTOMIZAÇÃO DA SOLUÇÃO TECNOLÓGICA E FORMAÇÃO, CONTRATAÇÃO EFETUADA NO ÂMBITO DA INICIATIVA 12 DA OPERAÇÃO N.º POCI-05-5762-FSE-039376

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, 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, sendo a Segunda Contratante a entidade com a qual será assinado o contrato em questão.

Cláusula 2.ª
Objeto

1. O procedimento tem por objeto a celebração de um contrato misto de aquisição de uma solução de segurança da informação (*software*), a instalar *on-prem*, considerando uma subscrição inicial de 1 (um) ano, a um universo de 1.000 (mil) utilizadores, incluindo os serviços de instalação, implementação, customização da solução tecnológica e formação, de acordo com as especificações técnicas constantes da Parte II do presente Caderno de Encargos e do seu Anexo, respetivamente.

2. A aquisição ema preço tem enquadramento na Iniciativa 12 [Solução de segurança de informação] da Operação N.º POCI-05-5762-FSE-039376, cofinanciada pelo Fundo Social Europeu no âmbito do Portugal 2020.

Cláusula 3.ª
Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.

2. 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 e respetivos Anexos;

   d) A proposta adjudicada;

   e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.

4. 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 e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma legal.

Cláusula 4.ª
Prazo

O prazo de execução é, previsivelmente, de 3 (três) meses a contar da data da assinatura do contrato, com termo a 31/03/2021, que corresponde à data em que termina a Operação N.º POCI-05-5762-FSE-039376.

Cláusula 5.ª
Preço base

1. O preço base para o presente procedimento é **€ 74.950,00** (setenta e quatro mil, novecentos e cinquenta euros), acrescido de IVA à taxa legal em vigor de 23%, o que perfaz o montante total de **€ 92.188,50** (noventa e dois mil, cento e oitenta e oito euros e cinquenta cêntimos).

2. Por forma a dar cumprimento ao dever de fundamentação imposto no n.º 3 do artigo 47.º do CCP, informa-se que o preço foi estabelecido com base em critérios objetivos, tendo por referência um orçamento apresentado no âmbito da consulta preliminar efetuada ao mercado, nos termos do artigo 35.º-A do CCP, conforme descrito na Informação de suporte à abertura do presente procedimento.

3. Com vista a dar cumprimento aos n.ºs 2, 3 e 4 do artigo 35.º-A do CCP, informa-se que:

    a) A Divisão de Sistemas de Informação da ACT efetuou uma consulta preliminar ao mercado, nos termos do artigo 35.º-A do CCP, tendo solicitado orçamento à sociedade comercial *«Oramix Sistemas de Informação S.A.»* [NIPC: 504 448 382], com vista a auxiliar, exclusivamente, a tarefa de fixação e justificação do preço base do presente procedimento tendo por referência critérios objetivos (cf. n.º 3 do artigo 47.º do CCP);

    b) Por seu turno, a *«Oramix Sistemas de Informação S.A.»* apresentou orçamento no valor de € 74.950,00 (setenta e quatro mil, novecentos e cinquenta euros), acrescido de IVA à taxa legal em vigor de 23%, o que perfaz o montante total de € 92.188,50 (noventa e dois mil, cento e oitenta e oito euros e cinquenta cêntimos).

CAPITULO II

OBRIGAÇÕES CONTRATUAIS
Secção I – Obrigações do fornecedor do *software*

Subsecção I
Disposições Gerais

Cláusula 6.ª
Obrigações do fornecedor

1. Apresentar proposta em resposta ao convite formulado pela ACT, no âmbito do presente Caderno de Encargos e seu Anexo, com recurso à plataforma eletrónica acinGov.
2. A 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.
3. A entidade adjudicatária deverá cumprir a obrigação de assegurar a entrada em produção da solução no prazo máximo de 30 (trinta) dias consecutivos, contados desde a data da sua parametrização.
4. A entrada em produção da solução deverá ser assegurada, impreterivelmente, em data anterior a 31/03/2021, que corresponde ao termo da execução da Operação N.º POCI-05-5762-FSE-039376.
5. 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.
6. Não alterar as condições estabelecidas para o desenvolvimento do *software* fora dos casos previstos no presente Caderno de Encargos.
7. Prestar de forma correta e fidedigna as informações referentes às prestações que integram o objeto contratual, bem como prestar todos os esclarecimentos que se justifiquem.

8. 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.

9. 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
Requisitos técnicos e funcionais

O fornecedor obriga-se a cumprir os 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. Pelas prestações que constituem 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:

    c) 10% após o cumprimento da obrigação de disponibilização e parametrização da solução;

    d) 90% após o cumprimento da obrigação de assegurar a entrada em produção da solução.

2. As faturas só podem ser emitidas após o cumprimento das obrigações referidas no número anterior.

3. As faturas 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.

4. O não pagamento total das faturas 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 das faturas atá ao dia, inclusive, em que o pagamento integral desse montante seja efetuado na conta bancária do segundo outorgante.

5. Em caso de discordância por parte da ACT, quanto ao valor indicado nas faturas, 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, cada fatura é paga 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.

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 Código dos Contratos Públicos.

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 Código dos Contratos Públicos.

CAPITULO III
PENALIDADES E RESCISÃO CONTRATUAL

Cláusula 16.ª
Penalidades contratuais

1. Pelo incumprimento dos prazos fixados para o cumprimento das 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 prazo fixado para a disponibilização da licença, 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/365

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 Código dos Contratos Públicos.

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 Código dos Contratos Públicos.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Cláusula 21.ª
Entrada em vigor

1. O contrato produz efeitos desde a data da sua assinatura até 31/03/2021.

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 Código dos Contratos Públicos, 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 471º do CCP.

Cláusula 24.ª
Casos omissos

Em tudo o omisso no contrato observar-se-á o disposto no Código dos Contratos Públicos, aprovado pelo Decreto-Lei nº 18/2008, de 29 de janeiro, com as posteriores alterações legais, 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 mais 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. Assim, 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.

9. 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 colaboradores da ACT.

10. Deste modo e no âmbito do projeto SAMA, o e-ACT, enquadra-se a aquisição de uma solução que concretiza a componente de segurança de informação e a conformidade com o RGPD.

11. De modo a monitorizar e operacionalizar o Sistema de Gestão de Segurança da Informação, houve a necessidade de proceder à análise de uma solução que garanta a segurança de informação, através da análise e automação de processos (utilizadores e grupos, classificação de informação, permissões, acessos, entre outros) e que assegure a privacidade, governação, deteção e respostas a eventuais ameaças e a rastreabilidade de acessos a toda a informação constante nos servidores de ficheiros da ACT, repositórios de correio eletrónico (*Exchange*), VPN/DNS/WEB, *Teams*, *Sharepoint*, entre outros.

Cláusula 26.ª
Requisitos da Solução Tecnológica

1. A solução deverá assegurar o cumprimento da RCM 41/2018, das políticas de segurança referentes ao sistema de Gestão de Segurança de Informação da ACT e o correto funcionamento do RGPD, designadamente:

   a) Monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis;

   b) Proteção dos dados contra modificações não autorizadas, perdas, furtos e divulgação não autorizada;

   c) Monitorizar os ficheiros partilhados e revogar o acesso, se for necessário e no caso de ocorrerem eventos inesperados;

   d) Atribuição de direitos de acesso e privilégio de forma restrita e controlada;

   e) Capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados pessoais;

   f) Capacidade para garantir que os utilizadores façam uma utilização correta dos dados;

   g) Inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional;

   h) Classificar automaticamente a informação armazenada no que diz respeito a dados pessoais;

   i) Configurar políticas para classificar e etiquetar manualmente os dados com base na confidencialidade e, em seguida, aplicar uma proteção persistente;

   j) Disponibilizar relatórios para monitorizar e compreender as violações e cumprimento de políticas impostas;

k) Deteção de ameaças e alertas de possíveis incidentes de segurança.

l) No entanto, a solução deverá responder na íntegra aos requisitos técnicos para regular a aquisição da Solução de Segurança da Informação que se encontram especificados no documento em anexo e contemplar todos os utilizadores e unidades orgânicas da ACT.

2. A ACT pretende adquirir 1.000 (mil) licenças, em regime de subscrição válida por 1 (um) ano, para constituir a Solução de Gestão de Segurança da Informação da ACT, a instalar *on-prem*, incluindo os serviços de instalação, implementação, customização da solução tecnológica e formação.

3. A Solução de Segurança de Informação deverá respeitar as funcionalidades e as especificações técnicas constantes em Anexo ao presente Caderno de Encargos.

Cláusula 27.ª
Prazo para Disponibilização e Parametrização da Solução

A 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.

Cláusula 28.ª
Prazo para Entrada em Produção da Solução

1. A entidade adjudicatária deverá cumprir a obrigação de assegurar a entrada em produção da solução no prazo máximo de 30 (trinta) dias consecutivos, contados desde a data da sua parametrização.

2. A entrada em produção da solução deverá ser assegurada, impreterivelmente, em data anterior a 31/03/2021, que corresponde ao termo da execução da Operação N.º POCI-05-5762-FSE-039376.

Cláusula 29.ª
Local de faturação

As faturas devem ser enviadas 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.

ANEXO

REQUISITOS TÉCNICOS SOLUÇÃO DE SEGURANÇA DE INFORMAÇÃO

1. OBJETO E ÂMBITO

Por forma a garantir o correto cumprimento do RGPD, em sede do presente Anexo são definidos os requisitos técnicos da solução tecnológica de segurança de informação.

A contratação visa:

- Implementar uma solução tecnológica (*software*), *on-prem*, para cumprimento regulamentar do RGPD.
- Formação e suporte técnico na solução tecnológica.

2. IMPLEMENTAÇÃO DE SOLUÇÃO TECNOLÓGICA (SOFTWARE)

A solução tecnológica, a instalar *on-prem*, deve considerar uma subscrição inicial de 1 ano, a um universo de 1.000 utilizadores do *Active Directory* da ACT, utilizadores simultâneos e servidores de ficheiros (*Windows* e *Sharepoint*), bem como obedecer a uma série de características e funcionalidades listadas a seguir.

2.1. GESTÃO DA SEGURANÇA DOS DADOS AUDITADOS

A solução proposta deve permitir a administração de permissões para os servidores monitorizados. Entre as quais:

- Permitir a gestão unificada de todos os ambientes auditados a partir de uma única consola.
- Permitir a auditoria das permissões de acesso a pastas partilhadas na rede. O sistema deve ser capaz de diferenciar as permissões NTFS das permissões partilhadas na rede.
- Permitir uma fácil gestão das permissões de acesso, e incluir uma funcionalidade de simulação para poder fazer alterações sem

afetar as permissões definidas em produção.

- Permitir a identificação gráfica, e por relatórios, das pastas afetadas por inconsistências nas permissões.
- Alerta de falhas na aplicação das permissões caso seja detetada uma inconsistência na rota afetada pela alteração.
- Permitir a análise das estatísticas de acesso de cada utilizador aos diferentes recursos auditados.
- A solução deve permitir pesquisas bidireccionais para acesso com base em utilizadores, dados ou uma combinação de ambos.
- A ferramenta deve fornecer recomendações sobre permissões e grupos com base na atividade e tipo de atividade, como por exemplo, a eliminação de utilizações ou permissões inativas sobre os recursos dos servidores monitorizados. O intervalo de inatividade dos recursos inativos deve ser customizável ao longo do tempo.
- A ferramenta também deve incluir a capacidade de atribuir um potencial proprietário da informação a cada pasta do sistema para permitir uma fácil monitorização da pasta, bem como a capacidade de configurar um relatório automático dessa atividade. A atribuição do referido proprietário também deve poder ser realizada em massa, através de arquivo predefinido.
- Toda a atividade realizada a partir da consola na gestão de permissões deve ser registada pela solução proposta, permitindo as seguintes funcionalidades:
    - Revisão das alterações propostas com base nas funções de revisão e autorização.
    - Permitir o *rollback* dos processos à situação anterior à mudança.
    - Permitir o planeamento da implementação de alterações

numa data e hora específicas.

- Permitir a elaboração de relatórios regulares e notificação automática por e-mail.

- Permitir a pesquisa e relatórios das ações realizadas pela consola Varonis identificando o operador que as realizou e os objetos afetados pela alteração.

- Todas as alterações feitas às permissões devem permitir comparações da nova configuração com a configuração anterior à mudança.

2.2. AUDITORIA DA ATIVIDADE DE ACESSO

A solução tecnológica deve ter o controlo de todos os acessos às informações geradas pelos servidores monitorizados, bem como ser capaz de auditar e consultar todos os *logs* de acesso aos ficheiros contidos nas pastas partilhadas. Para o fazer, a solução deve ter as seguintes funcionalidades:

- Possuir uma auditoria exaustiva de todos os eventos de acesso às informações contidas nas pastas partilhadas: ficheiro aberto, modificado, apagado, movido, renomeado ou pasta aberta, modificada, apagada, movida ou renomeada, bem como as alterações de permissões feitas nas pastas monitorizadas.

- Ter o seu próprio agente e não depender da auditoria nativa do Windows.

- Propor um sistema de armazenamento desses *logs*, baseado numa base de dados SQL compatível com a arquitetura SQL fornecida pelo cliente. Esta base de dados irá também alojar a configuração do sistema proposto.

- Ter um sistema central de pesquisa de *logs* que permite pesquisar os *logs* das pastas partilhadas. Além disso, a pesquisa deve ser ágil, e a solução deve propor a possibilidade de pesquisar e filtrar os *logs* gerados por um utilizador específico, sobre um recurso

específico, durante um determinado período de tempo, etc.

- Ter a possibilidade de exportar os resultados de uma pesquisa para uma folha *Excel* ou um *PDF*, rápida e diretamente, bem como oferecer um sistema de *reporting* personalizável nas informações fornecidas.

- Permitir a geração de pesquisas personalizadas, armazená-las e reutilizá-las sem a necessidade de as configurar.

2.3. ADMINISTRAÇÃO DAS LICENÇAS DE SEGURANÇA AUDITADAS

A solução tecnológica deve permitir que seja realizada a administração das permissões dos servidores monitorizados. Entre eles, deve permitir:

- Gestão unificada de todos os ambientes a partir de uma única consola.

- Gestão e proteção do *Active Directory* em ambientes multi-domínio, a partir de uma única consola.

- Auditoria de permissões de acesso a pastas partilhadas na rede. Deverá ser capaz de diferenciar permissões NTFS, permissões partilhadas e permissões *Sharepoint* se estas últimas forem monitorizadas, tanto nas versões *On Premise* como no Office 365.

- A gestão das permissões de acesso é feita de forma simples, e inclui uma funcionalidade de simulação para poder fazer alterações sem afetar as permissões definidas em produção.

- Que todas as operações de alteração de permissão sejam registadas na aplicação para revisão, aprovação, aplicação imediata ou agendada e com a possibilidade de reversão no caso de se querer desfazer a alteração.

- A criação e eliminação de diferentes elementos do *Active Directory* através da interface de controlo, individualmente ou em massa, com base em fontes de informação.

- A análise das estatísticas de acesso de cada utilizador aos diferentes recursos auditados.

- Fornecer recomendações sobre permissões e grupos com base na atividade e tipo de atividade, recomendando por exemplo a eliminação de utilizações inativas ou permissões inativas sobre os recursos dos servidores monitorizados. O intervalo de inatividade dos recursos inativos deve ser personalizável ao longo do tempo.

- A capacidade de atribuir a cada pasta do sistema um potencial proprietário da informação, para permitir uma monitorização fácil da pasta, bem como a capacidade de auto-reporting dessa atividade ao proprietário.

2.4. CLASSIFICAÇÃO DA INFORMAÇÃO

A solução tecnológica será capaz de localizar, marcar ou apagar os dados pessoais de uma forma geral, e sobre um utilizador específico. Por conseguinte, a solução deve:

- Ter um sistema de classificação da informação para detetar os Dados Pessoais de cidadãos da União Europeia e dados relativos a PCI (*Payment Card Information* – dados de cartões de pagamento), bem como os dados pessoais na acepção dada pelo RGPD.

- Permitir a classificação da informação em ficheiros do Office, ficheiros PDF, ficheiros de texto simples, bem como a classificação com base em extensões de ficheiros, por exemplo, ficheiros multimédia.

- Ser capaz de examinar as permissões nas pastas que contêm informações pessoais para avaliar o risco associado.

- Permitir a criação de padrões específicos para pesquisar algumas expressões regulares. Estas expressões podem corresponder a dados pessoais dum utilizador específico, ou pode ser uma palavra específica que possa corresponder a um projeto sensível do cliente. Esta customização deve também permitir a

incorporação de dicionários personalizáveis sobre assuntos gerais ou aqueles definidos pelo cliente.

- Ter uma classificação que será refletida nos dados como uma *tag/flag* adicional de metadados, integrável com outras soluções de segurança via API ou algum conetor.

- Permitir a opção de poder importar automaticamente informações de classificação de outros sistemas, tais como DLP, e incorporá-las na gestão de classificação da solução.

2.5. ALERTAS

A solução tecnológica detetará potenciais ameaças que possam afetar a informação, as violações de segurança e alertar sobre estes problemas em tempo real. Por conseguinte, a solução tem de:

- Ter a capacidade de emitir alertas de comportamento com base em eventos em excesso, alterações de atividade ou acessos não habituais a pastas inativas. Além disso, estes alertas devem ter em conta a classificação da informação previamente detalhada, a fim de fornecer alertas sobre incidentes em informação de carater pessoal.

- Ter alertas predefinidos que permitam agir contra as ameaças de ciberataque mais comuns, bem como a possibilidade de atualizar e alargar estes alertas à medida que a solução evolui.

- Proteger o *Active Directory* contra ataques cibernéticos, tendo a capacidade de detetar e bloquear pelo menos as seguintes ameaças:

    - Deteção de escalada de privilégios, através da modificação da associação a grupos com privilégios elevados.

    - Deteção de múltiplas tentativas de login e bloqueio contra ataques *pass the hash*.

    - Deteção de tentativas de login em contas desabilitadas.

- Deteção de delegação de autenticação com *Kerberos Ticket* (*Golden ticket*).
- Deteção de logins de conta de serviço a partir de laptops ou dispositivos móveis.
- Deteção de ataque de força bruta em arranque massivo de sessões.
- Logins de conta de utilizador a partir de dispositivos incomuns.
- DoS (*Denial of Ser*vice) devido à eliminação massiva de objetos do Active Directory.
- Modificação de associação a grupos críticos de administração do *Active Directory*.
- *Identificação das contas furtivas no Active* Directory (com menos de 1 dia de antiguidade).
- Modificação das configurações de segurança das políticas de grupo do *Active Directory*.

- Permitir a criação de alertas personalizados com base no tipo de evento gerado, na quantidade de eventos gerados durante um determinado período de tempo, no utilizador que gerou o evento, quando o evento ocorreu, qual o objeto do sistema de ficheiros que foi afetado pela alteração (servidor, pasta, *path*, tipo de ficheiro, etc.) e em que período de tempo.
- Converter um alerta numa mensagem do tipo "*syslog*", SNMP ou em executável.
- Enviar alertas e relatórios por *e-mail*.
- Permitir o armazenamento dos registos gerados durante um período de tempo flexível e configurável numa base de dados específica.

- Atuar na deteção do alerta através de *Powershel*l obtendo de forma simples as variáveis do script dos eventos que geraram o alerta. Como exemplo, desativará automaticamente um utilizador caso este tenha atividades suspeitas detetadas pelo sistema de alerta.

- Ter uma análise comportamental dos utilizadores para detetar desvios: incluir modelos de ameaça pré-definidos para detetar e interromper certas ações. Por exemplo, detetar tentativas de conexão anormais, tentativas de acesso a pastas contendo ficheiros com informação pessoal, tentativas de roubo ou de fuga de informação, comportamento anormal por parte de administradores, ataques de *ransomware*, cópia massiva de ficheiros com informação pessoal, etc.

- Evitar, tanto quanto possível, falsos positivos, contas administrativas ou de serviços com padrões diferentes devem poder ser tratadas, para que os alertas sejam adaptados ao comportamento típico.

- Permitir a definição de perfis de utilizador para que os alertas respondam de forma diferente, com base nesses perfis. Os perfis devem permitir a identificação de contas administrativas, contas de serviço e contas que tratam de informação crítica do cliente.

2.6. PRODUÇÃO DE RELATÓRIOS

A solução tecnológica deve ter a capacidade de customização e geração de relatórios com as seguintes funcionalidades:

- Gerar relatórios sobre os registos gerados pelos utilizadores de sistemas de ficheiros, as permissões dos utilizadores em pastas e ficheiros, a lista de pastas e permissões de acesso dos utilizadores às pastas, a associação dos utilizadores a certos grupos de segurança do *Active Directory*, obsolescência de recursos, atividade dos utilizadores em vários elementos do sistema de ficheiros e tendências do sistema de ficheiros (atividade, crescimento de dados, permissões, etc.).

- Permitir a customização dos relatórios, de modo a que possam ser gerados relatórios adaptados à gestão do cliente.
- Propor relatórios executivos que permitam ver os resultados da classificação, os diferentes alertas em curso no sistema e os diferentes resultados dos alertas ao longo do tempo, etc.
- Permitir a geração de relatórios em vários formatos: Excel, PDF, XML, CSV...
- Permitir o agendamento e envio automático de relatórios por correio eletrónico ou armazená-los numa pasta local ou num recurso de rede.
- Além disso, os relatórios devem incluir:
    - Utilizadores inactivos no sistema.
    - Utilizadores habilitados e sem atividade.
    - Utilizadores que têm atalhos para pastas.
    - Utilizadores que têm uma palavra-passe que não expira.
    - Pastas que não foram acedidas por um período customizável.
    - Grupos de segurança vazios.
    - Grupos de segurança com utilizadores desabilitados.
    - Permissões inconsistentes.
    - Permissões de grupo globais: Todos/*Everyone*, utilizadores do domínio/*domain users*, etc.

2.7. AUTO-AVALIAÇÃO

A solução tecnológica deve permitir a realização de avaliações de risco, periódicas e quantificadas, sobre as diferentes ameaças a que a informação está exposta. Por conseguinte, a solução deve ter a capacidade de realizar análises de risco rapidamente, podendo programar-se os relatórios de análise de risco sobre dados de nível elevado e de carater pessoal.

2.8. DASHBOARD

A solução tecnológica deve ter um Painel de Controlo/*Dashboard* com as seguintes funcionalidades:

- Apresentação de alertas de acordo com:
  - Utilizadores que geram mais alertas.
  - Equipas que geram mais alertas.
  - Tipos de alertas mais gerados.
  - Ativos afetados pelos ataques de alerta gerados.
- Análise dos alertas detetados, sendo capaz de identificar:
  - Causa.
  - Problema detetado.
  - Forma de resolução.
- Apresentação de KPIs de monitorização, com as seguintes funcionalidades:
  - Percentagem de cumprimento.
  - Escala temporal de cumprimento.
  - Possibilidade de customização de KPIs (Agregar, Remover).

- Possibilidade de adicionar KPIs de monitorização a partir das seguintes plataformas:
    - Servidores CIFS: Windows, Netapp, EMC, Hitachi, HP…
    - *Active Directory*.
    - Servidor *Exchange*.
    - *Sharepoint On Premise*.
    - *Sharepoint Online*.
    - OneDrive.
    - Conformidade com RGPD.

2.9. OUTRAS CARATERÍSTICAS

A solução tecnológica também deve ter as seguintes funcionalidades:

- Ter um cliente que possa ser instalado nos postos de trabalho dos administradores, sem necessidade de acesso remoto ao servidor.
- *Conservar os* logs gerados pelos utilizadores durante um período flexível e configurável pelo cliente numa base de dados específica, bem como dispor de um sistema de arquivo e recuperação que permita gerir de forma otimizada o armazenamento e o histórico da informação coletada.
- Sistema de auto-vigilância da própria solução que detete:
    - Falhas da auditoria dos servidores monitorizados.
    - Falta de espaço na base de dados da solução.

2.3. FORMAÇÃO E APOIO TÉCNICO SOBRE A SOLUÇÃO TECNOLÓGICA

O adjudicatário selecionado deve prestar os seguintes serviços, no âmbito do contrato:

- Serviço de formação:
  - Realização de um curso presencial sobre a solução tecnológica para auditoria e segurança de dados aos colaboradores do cliente que tenham o perfil de administrador da solução.
  - Este curso será realizado, uma vez implementada a solução tecnológica, e deverá incluir toda a informação teórica e prática exigida pelo perfil do administrador.
  - Os serviços de formação devem ser prestados nas instalações da ACT em Lisboa, oportunamente a definir.
- Serviço de suporte técnico via telefone e remoto em caso de possíveis incidentes com a solução tecnológica.