INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL, IP

CADERNO DE ENCARGOS

CONCURSO PÚBLICO SEM PUBLICAÇÃO NO JORNAL OFICIAL DA UNIÃO EUROPEIA (JOUE) Nº PR2021210/270

AQUISIÇÃO DE SOLUÇÃO INTEGRADA PARA A REALIZAÇÃO DE BACKUPS CYBER RECOVERY

PARTE I

CLAÚSULAS JURÍDICAS

Cláusula 1.ª
Objeto

O presente concurso tem por objeto a aquisição de Solução Integrada para realização de backups, com vista à proteção de dados e Cyber Recovery, do Instituto do Emprego e Formação Profissional, IP, (IEFP, IP), compreende as cláusulas a incluir nos contratos a celebrar, sendo adotado o procedimento de Concurso Público sem Publicação no Jornal Oficial da União Europeia, ao abrigo do disposto na alínea b) do n.º 1 do artigo 20.º do Decreto-Lei n.º 18/2008, de 29 de janeiro, alterado e republicado pelo Decreto Lei 111-B/2017, de 31 de agosto, doravante designado por CCP.

Cláusula 2.ª
Local da prestação dos serviços

Os serviços, alvo do presente concurso, serão prestados nas instalações dos Serviços Centrais do Instituto do Emprego e Formação Profissional, I.P. (IEFP, I.P.), localizadas na Rua de Xabregas, n.º 52, em Lisboa.

Cláusula 3.ª
Duração do contrato

O contrato terá a duração prevista de trê anos, com data prevista de início a 01 de outubro de 2021 e terminus a 30 de setembro de 2024.

Cláusula 4.ª
Preço base

1. O preço contratual ou preço base é de **198.500,00€** (cento e noventa e oito mil e quinhentos euros), acrescido do valor do IVA à taxa em vigor.
2. O valor do preço base inclui todos os custos (equipamentos, instalação, manutenção e suporte por 3 anos), bem como todos os encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante.

Cláusula 5.ª
Condições de pagamento

1. O pagamento deverá ser efetuado de acordo com o abaixo discriminado:
   - Equipamentos: Pago após a entrega
   - Serviços de instalação: Pago após instalação concluída
   - Licenciamento: Pago após adjudicação
   - Serviços de manutenção: Pago anualmente
1. Se o adjudicatário se encontrar em condições de cumprir com o legalmente estipulado quanto à faturação eletrónica em procedimentos aquisitivos de contratação pública, nos termos e ao abrigo do disposto no Decreto-Lei n.º 28/2019, de 15 de fevereiro – artigo 12.º e 14.º - faturação por via eletrónica, que regula as obrigações relativas ao processamento de faturas e outros documentos

fiscalmente relevantes, e no Decreto-Lei n.º 123/2018, de 28 de dezembro, que define o modelo de governação para a implementação da faturação eletrónica nos contratos públicos, a fatura deverá ser compatível com o sistema de faturação eletrónica implementado pelo IEFP, I.P.

2. O pagamento de qualquer fatura está dependente do cumprimento, por parte do adjudicatário do previsto no presente caderno de encargos, bem como do conhecimento da situação tributária e contributiva do mesmo.
3. Em caso de discordância por parte da entidade adjudicante, quanto aos valores indicados na fatura, deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. A entidade adjudicante efetuará o pagamento da fatura ao adjudicatário, num prazo não superior a 30 (trinta) dias, a partir da data da sua entrada nos seus serviços.
5. Na eventualidade do não cumprimento do prazo referido no número anterior, aplicar-se-á a Lei n.º 3/2010, de 27 de abril, que estabelece a obrigatoriedade do pagamento de juros de mora, calculados à taxa legal em vigor.
6. Nas condições de pagamento a apresentar pelo concorrente não podem ser propostos adiantamentos por conta dos bens a fornecer.
7. O pagamento de quaisquer valores apresentados apenas será efetuado após aceitação dos equipamentos, a que se referem esses valores.

Cláusula 6.ª

Obrigatoriedade da Faturação Eletrónica

1. De acordo com a Diretiva 2014/55/EU e Decreto-Lei 123/2018, de 28 de dezembro, a partir de 18 de abril de 2020 a entidade adjudicante fica obrigada a receber faturas eletrónicas no modelo a que se refere o n.º 3 do artigo 299.º-B do Decreto-Lei 111-B/2017 de 31 de agosto.
2. Até 31 de dezembro de 2020, os cocontratantes podem utilizar mecanismos de faturação diferentes dos previstos pelo artigo 299.º-B do Decreto-Lei 111-B/2017, de 31 de agosto, tornando-se obrigatória a sua utilização a partir desse momento.
3. O prazo estabelecido pelo número anterior é alargado para 30 de junho de 2021 no caso de pequenas e médias empresas e 31 dezembro de 2021 para as microempresas de acordo com os prazos estabelecidos pelo Decreto-Lei n.º 14-A/2020.
4. A entidade adjudicante poderá antecipar os prazos legais de receção de faturas eletrónicas, através de comunicação formal via email, pelo que o adjudicatário deverá cumprir com os prazos definidos.
5. O modelo integrado de receção de faturação eletrónica adotado pela entidade adjudicante é o EDI (Intercâmbio Eletrónico de Dados), sendo que o adjudicatário deverá enviar as suas faturas eletrónicas através de interligação dos seus softwares de faturação com o Portal FE AP da ESPAP.

Cláusula 7.ª

Obrigações de Sigilo

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
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 previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário 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.
4. O adjudicatário obriga-se a manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenha no âmbito da formação e da execução do contrato, nem utilizar as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos.
5. O adjudicatário compromete-se a tomar as medidas necessárias para que os seus agentes, funcionários, colaboradores ou terceiros envolvidos na execução do contrato se vinculem à obrigação de confidencialidade referida no número anterior.

Cláusula 8.ª

Proteção de Dados

1. O adjudicatário é obrigado a tratar todos os dados pessoais a que tiver acesso, de acordo com o previsto no Regulamento Geral de Proteção de Dados Pessoais aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), devendo, nomeadamente:
2. Tratar os dados pessoais apenas mediante instruções documentadas da entidade adjudicante, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso a entidade adjudicante desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;
3. Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
4. Adotar todas as medidas exigidas nos termos do artigo 32.º do RGPD;
5. Garantir o cumprimento do RGPD, nas condições aqui previstas, quando pretenda contratar um subcontratante;
6. Tomar em conta a natureza do tratamento, e na medida do possível, prestar assistência à entidade adjudicante pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos direitos previstos no capítulo III do RGPD;
7. Prestar assistência à entidade adjudicante no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º do RGPD, tendo em conta a natureza do tratamento e a informação ao seu dispor;
8. Consoante a escolha da entidade adjudicante, apagar ou devolver-lhe todos os dados pessoais depois de concluído o contrato, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros;
9. Disponibilizar à entidade adjudicante todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na presente cláusula, facilitando e contribuindo para as auditorias, inclusive as inspeções, conduzidas pela entidade adjudicante ou por outro auditor por esta mandatado.

10. O não cumprimento do RGPD, por facto imputável ao adjudicatário, é considerado, para todos os efeitos, incumprimento definitivo, podendo a entidade adjudicante resolver o contrato, ao abrigo da alínea a) do n.º 1 do artigo 333.º do CCP.
11. O adjudicatário será responsável por qualquer prejuízo em que a entidade adjudicante venha a incorrer em consequência do tratamento dados pessoais em violação das normas legais aplicáveis e/ou do disposto no contrato, desde que tal que lhe possa ser imputável.
12. Compete ao adjudicatário informar imediatamente a entidade adjudicante se alguma instrução violar o contrato celebrado, o Regulamento Geral de Proteção de Dados ou quaisquer outras disposições legais nacionais ou europeias em matéria de proteção de dados.
13. O adjudicatário autoriza a entidade adjudicante ao tratamento dos dados pessoais necessários no âmbito das diligências prévias à formação do contrato bem como no decurso e para efeitos da execução do mesmo, comprometendo-se a obter, caso se aplique, o prévio consentimento expresso dos titulares dos dados respetivos.
14. O adjudicatário autoriza a entidade adjudicante ao tratamento dos dados pessoais necessários no âmbito da publicitação dos contratos no portal Base.GOV.

Cláusula 9.ª

Obrigações do adjudicatário

1. O adjudicatário obriga-se a prestar os serviços ao IEFP, I.P., nos termos das disposições do presente caderno de encargos, de acordo com a respetiva proposta e com as orientações e recomendações técnicas recebidas.

2. Sem prejuízo do referido no número anterior constituem, designadamente, obrigações do adjudicatário:

a) Obrigação de elaboração de relatórios referentes à prestação dos serviços, quando solicitado pelo IEFP, I.P.;

b) Obrigação de prestação de informação e/ou esclarecimentos, relativamente aos serviços e ao cumprimento das obrigações emergentes do contrato, quando solicitado pelo IEFP, I.P., e com a periodicidade que for julgada necessária;

c) A obrigação prevista na alínea anterior compreende o dever de o adjudicatário participar em reuniões com o IEFP, I.P., ou com quem este vier a designar;

d) Obrigação de submissão a fiscalização por parte do IEFP, I.P., ou outra entidade que este designar.

Cláusula 10.ª

Cessão da posição contratual

1. O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da entidade adjudicante.
2. Para efeitos da autorização prevista no número anterior, deve:
   a. Ser apresentada pelo cessionário toda a documentação exigida ao adjudicatário no presente procedimento;
   b. A entidade adjudicante apreciar, designadamente, se o cessionário não se encontra em nenhuma das situações previstas no artigo 55.º do CCP.

Cláusula 11.ª

Subcontratação

O adjudicatário não poderá, por qualquer forma, subcontratar terceiras entidades para a realização de tarefas relativas ao objeto do contrato, sem prévio consentimento da entidade adjudicante.

Cláusula 12.ª

Casos Fortuitos ou de Força Maior

1. Não podem ser impostas penalidades ao adjudicatário, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes 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 fosse razoavelmente exigível contornar ou evitar.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
    a. Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;
    b. Greves ou conflitos laborais limitados às sociedades do adjudicatário ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
    c. Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo adjudicatário de deveres ou ónus que sobre ele recaiam;
    d. Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;
    e. Incêndios ou inundações com origem nas instalações do adjudicatário cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
    f. Avarias nos sistemas informáticos ou mecânicos do adjudicatário não devidas a sabotagem;
    g. 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.

Cláusula 13ª

Patentes, Licenças e Marcas

1. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização no fornecimento, de marcas registadas, patentes registadas ou licenças.
2. Caso a entidade adjudicante venha a ser demandada por alegadamente ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o adjudicatário indemniza-o de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.

Cláusula 14.ª

Contrato

1. Fazem sempre parte integrante do contrato, independentemente da sua redução a escrito:
   a. Os suprimentos 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 prestada pelo adjudicatário.
2. Em caso de discrepância entre os vários elementos que compõem o contrato, prevalece a ordem por que vêm enunciados no número anterior.
3. O adjudicatário obriga-se a entregar os seguintes documentos de habilitação, no prazo de 5 dias uteis após a notificação adjudicação:
   a. Declarações emitida conforme modelo constante do anexo II ao programa de concurso;
   b. Documento comprovativo que não se encontrem nas situações previstas na alínea b), d), e) e h) do nº 1 do art.º 55º do Código dos Contratos Públicos;
   c. Fotocópia do cartão de contribuinte ou do cartão de pessoa coletiva, conforme os casos;
   d. Certidão do registo comercial, onde conste a matrícula e todas as inscrições em vigor, nomeadamente a forma de obrigar;
   e. Catálogos e demais documentações, em língua portuguesa, relativo aos equipamentos a fornecer.
4. A entidade adjudicante pode excluir expressamente do contrato os termos ou condições constantes da proposta adjudicada que se reportem a aspetos da execução do contrato não regulados pelo caderno de encargos e que não sejam considerados estritamente necessários a essa execução ou sejam considerados desproporcionados.

Cláusula 15.ª

Interpretação do Contrato

1. Em caso de dúvida sobre a interpretação das regras aplicáveis à execução do contrato, o adjudicatário deve solicitar por escrito um esclarecimento à entidade adjudicante.
2. O adjudicatário obriga-se a ter em conta, as orientações que lhe forem transmitidas por escrito pela entidade adjudicante.

Cláusula 16.ª

Resolução do contrato

1. O contrato pode ser resolvido por qualquer das partes em caso de incumprimento definitivo, grave ou reiterado, e culposo por uma das partes das obrigações por si assumidas no contrato, nos termos gerais de direito, sem prejuízo das correspondentes indemnizações legais a que houver lugar.
2. Para efeitos do disposto no número anterior, a parte não culposa comunicará por escrito a ocorrência da situação de incumprimento suscetível de gerar resolução contratual, concedendo à contraparte um prazo não inferior a 10 (dez) dias para que aquela reponha a situação de incumprimento, sem o que, o incumprimento se tornará definitivo e determinará a resolução contratual, nos demais termos gerais de direito.

3. O contrato pode também ser resolvido através da entidade adjudicante caso se verifique alguma das seguintes situações, as quais são desde já entendidas como situações de incumprimento grave e culposo por parte do adjudicatário:
   a. Quando não se verificar a disponibilização e instalação dos equipamentos acordados nas datas fixadas pelas partes, por causa direta e exclusivamente imputável ao adjudicatário;
   b. Quando se verificar reiterada inobservância das disposições do contrato ou má-fé do adjudicatário;
   c. Prestação de falsas declarações;
   d. Estado de falência ou insolvência;
   e. Cessação da atividade;
   f. Condenação, por sentença transitada em julgado, por infração que afete a idoneidade profissional do fornecedor e desde que não tenha ocorrido reabilitação judicial.

4. O direito de resolução referido no número anterior exerce-se mediante declaração escrita enviada ao adjudicatário.

Cláusula 17.ª
Gestor do Contrato

No clausulado do contrato será indicado o gestor do contrato em nome da entidade adjudicante nos termos do artigo 290º-A, do CCP.

Cláusula 18.ª
Responsabilidade do Adjudicatário

1. O adjudicatário responde pelos danos que causar à entidade adjudicante em razão do incumprimento culposo das obrigações que sobre ele impendam.
2. O adjudicatário responde ainda perante a entidade adjudicante pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações assumidas, como se tais atos ou omissões fossem praticados por aquele.

Cláusula 19.ª
Despesas

Correm por conta do adjudicatário, todas e quaisquer despesas, nomeadamente as de deslocação e estadia, em que este haja de incorrer em virtude da execução das obrigações que para aquele emerjam do presente Caderno de Encargos e do contrato.

Cláusula 20.ª
Prevalência

1. Fazem parte integrante da relação contratual o caderno de encargos, os esclarecimentos e a proposta do adjudicatário.
2. Em caso de dúvida prevalece em primeiro lugar o caderno de encargos, seguidamente os esclarecimentos e por último a proposta do adjudicatário.

Cláusula 21.ª
Lei Aplicável

O contrato rege-se pela lei portuguesa.

Cláusula 22ª
Foro Competente

Para todas as questões emergentes do contrato será competente o Tribunal Administrativo de Círculo de Lisboa.

PARTE II

CLÁUSULAS TÉCNICAS

CARACTERÍSTICAS DA PRESTAÇÃO DE SERVIÇOS

Cláusula 23.ª
Objeto

1. O presente cadeno de encargos tem por objeto a aquisição de Solução Integrada para realização de backups, com vista à proteção de dados e Cyber Recovery, ao Instituto do Emprego e Formação Profissional, IP, (IEFP, IP).
2. Em concreto, pretende-se a aquisição de uma solução de proteção de dados totalmente integrada e convergente ao nível de software, hardware, pesquisa e analítica, em formato de appliance e que permita endereçar as seguintes necessidades, cumprindo na integra com os requisitos técnicos identificados nas cláusulas que se seguem.

Cláusula 24.ª
Requisitos genéricos

Pretende-se a aquisição de uma solução de proteção de dados totalmente integrada e convergente ao nível de software, hardware, pesquisa e analítica, em formato de appliance e que permita endereçar as seguintes necessidades, cumprindo na integra com os requisitos identificados:

1. Solução de Proteção de Dados

A solução de proteção de dados a propor deverá permitir ao IEFP, IP acomodar as necessidades atuais de proteção de dados, bem como garantir o seu crescimento de forma fácil e transparente. A solução a propor deverá ter em consideração os elevados requisitos de Recovery Point Objective e Recovery Time Objective das aplicações críticas, bem como a garantia de recuperabilidade dos dados armazenados na solução de proteção de dados, tanto a partir de desastres como de ciberataques.

1.1 Licenciamento da solução de proteção de dados:

- O licenciamento da solução de proteção de dados a propor deverá permitir ao IEFP acomodar as suas necessidades de proteção de dados, bem como continuar a garantir o seu crescimento de forma fácil e transparente. O licenciamento a propor deverá ter em consideração os elevados requisitos de Recovery Point Objective e Recovery Time Objective das aplicações críticas, bem como a garantia de recuperabilidade dos dados armazenados na solução de proteção de dados.

1.2 **Pretende-se a aquisição de um licenciamento totalmente flexível por forma a permitir um melhor enquadramento na realidade da infraestrutura do IEFP, nomeadamente ao suporte da infraestrutura de virtualização**:

- Licenciamento ilimitado em termos de volume de dados a proteger, número de máquinas (físicos e/ou virtuais), independentemente do sistema operativo e/ou hipervisor, bem como a número de aplicações a proteger;
- Possibilidade de proteger máquinas físicas, incluindo bases de dados, não pertencentes à infraestrutura de virtualização;
- Possibilidade de proteger storage NAS;
- Possibilidade de proteger postos de trabalho (desktop/laptop);
- O licenciamento deverá permitir acomodar tanto as necessidades de backup, como de replicação, monitorização, analítica e pesquisa de metadados.
- A solução a propor deverá permitir a migração dos dados existentes no atual Dell Data Domain DD6300 para a nova solução, com recurso e mecanismos nativos de replicação entre o DD6300 e a nova solução a propor, sem recurso a restore, criação de 2ª cópia, rehidratação ou qualquer tipo de alteração dos dados atualmente armazenados.

1.3 Características e requisitos técnicos da solução de backup:

Entre outras funcionalidades, a solução de proteção de dados a adquirir deverá garantir:

- Suporte para tecnologia de deduplicação de dados inline e de bloco variável, para otimização dos rácios de deduplicação;
- A deduplicação entre sites e servidores, independentemente do tipo de dados;
- Backups rápidos e eficientes para todo o tipo de dados, independentemente da sua origem;
- A possibilidade de replicação eficiente ao nível de rede e suporte para vários métodos de replicação (1:1, n:1, 1:n);
- A replicação síncrona ou assíncrona, com granularidade ao nível de máquinas virtuais, permitindo selecionar o Recovery Point Objective pretendido;
- A possibilidade de exportar dados diretamente para cloud (publica e/ou privada), de forma fácil e transparente, garantindo o ownership dos metadados do lado on-premise e sem recurso a gateways externas;
- A capacidade de permitir a implementação de agentes de proteção de dados, para envio de dados diretamente a partir das aplicações (Hadoop, Microsoft SQL, Oracle, SAP, SAP HANA), para o repositório de proteção de dados, sem necessidade de software e equipamentos adicionais;
- Arquitetura desenhada por forma a garantir a integridade e recuperabilidade de todos os dados ingeridos e armazenados, com verificação de consistência do filesystem e capacidades de self-healing, por forma a prevenir, detetar e recuperar a partir de falhas de hardware ou software;
- Possibilidade de implementação de mecanismos de elevada segurança, que permitam garantir a invulnerabilidade da informação durante o ciclo de retenção dos dados, incluindo mecanismos de encriptação, sem recurso a discos auto-encriptáveis ou discos específicos para o efeito;
- Integração nativa, por intermédio do VMware vSphere Web Client, da componente de proteção de dados, incluindo as capacidades de gerir operações de backup, recuperação e de reporting do estado da proteção das máquinas virtuais;

- Capacidade de iniciar máquinas virtuais críticas, diretamente a partir da imagem de backup, sem necessidade de iniciar uma recuperação tradicional, por forma a reduzir ao máximo o Recovery Point Objective para minutos, independentemente do tamanho da máquina virtual;
- Capacidade de recuperação granular de máquinas virtuais, ao nível do VMDK, mantendo o formato de aprovisionamento do mesmo (thin provisioning);
- Arquitetura redundante ao nível de arrefecimento (N+1), fontes de alimentação hot-swappable, memória protegida por bateria (para acautelar contra a corrupção de dados em memória em caso de falha de energia ou do software), proteção de dupla paridade RAID6;
- A entrega de uma solução de proteção de dados, incluindo backup, replicação, recuperação, monitorização e analítica totalmente integrada em formato de appliance e suportada a partir de um único fabricante;

1.4 Solução de Recuperação contra Ciber Ataques:

- Por forma a retirar partido de equipamentos existentes e uma maior racionalização de custos e recursos, a solução deverá permitir a reutilização do atual Dell Data Domain DD6300 para o cofre, permitindo um mecanismo de replicação nativa entre a solução a propor para o Datacenter Central e a solução a propor para o cofre;
- Como o controlo e gestão da solução de ciberproteção deverá ser feito a partir do cofre, mantendo o isolamento lógico da rede de produção, a replicação deverá ser feita por mecanismos nativos entre o repositório da solução do Datacenter Central e Dell Data Domain DD6300, sem qualquer orientação ou conhecimento do software de proteção de dados do lado da produção;
- A solução deve combinar os benefícios do isolamento e da continuidade de negócios, minimizar o impacto de um ciberataque e fornecer uma maior probabilidade de sucesso na recuperação de sistemas críticos, alinhado às práticas descritas pelo Instituto Nacional de Segurança e Tecnologia (NIST);
- Garantir automação e fluxo de trabalho para 14 cópias “Gold” dos dados mais críticos do IEFP, para um segundo repositório o qual tem de replicar nativamente com a solução a propor para a Proteção de Dados do Datacenter Central e das delegações, para que os processos de negócios possam ser retomados após um ataque destrutivo.
- O processo de deteção deverá incidir sobre os vetores de ataque utilizados pelas ferramentas de malware, ransomware e criptoware, sem necessidade de recurso exclusivo a deteção de assinatura maliciosa, que obriga a uma atualização constante da solução para manter o sucesso dos índices de deteção de código malicioso.

  Adicionalmente deverá ser proposta uma solução de proteção contra ciber-incidentes, combinando os seguintes pilares de proteção e recuperação:

- **Planeamento e design**, por avaliação dos sistemas e aplicações críticas para o negócio, infraestrutura atual, tempo de recuperação contra ciberataques, objetivos de recuperação para adequar a implementação da solução. A incluir a criação de mapeamentos de dependências com a infraestrutura associada, metadados, etc.;
- **Isolamento e replicação**, com base no resultado da fase de planeamento e design, que permita implementar as condições necessárias para um cofre de recuperação contra ciber-incidentes;

- **Analítica**, por forma a salvaguardar o bom funcionamento e eficácia das ferramentas de segurança cibernáutica, sendo requerida a capacidade de alavancar esta capacidade para análise de vetores de ataque que permitam detetar possíveis comprometimentos da informação protegida;
- **Restauro e recuperação**, a seguir os padrões que a solução disponibiliza, acrescido de considerações especiais a aplicar conforme os cenários desenhados a montante, por plano de resposta a ciber-incidentes, incluindo auxílio na avaliação forence e de dano aos dados, preparação da recuperação a partir das imagens "Gold" das aplicações e binários de sistemas operativos, a culminar no retorno do ambiente de produção em curto espaço de tempo.

Cláusula 25.ª

Requisitos específicos

1. Aquisição de uma nova plataforma integrada e solução de proteção de dados

Deverá ser proposta uma nova plataforma totalmente integrada e convergente ao nível de software, hardware, pesquisa e analítica que ofereça uma solução de proteção de dados, capaz de permitir ao IEFP acomodar as necessidades de proteção dos volumes de dados atuais e respetivas taxas de crescimento, que contemple os seguintes requisitos mínimos:

1.1 Capacidade de proteção de dados no Datacenter Central do IEFP para um volume de dados estimado em:

- 27 TB de dados em ambientes virtualizados VMware, onde se incluem Bases de Dados SQL
- 3TB de dados em fileshares locais
- 2TB de dados em Bases de Dados SQL em storage partilhado

1.2 Capacidade de proteção de dados nas delegações do IEFP espalhadas pelo território nacional, estimado em:

- Até 3TB de dados em fileshares locais, por delegação

1.3 Política de backup consistente com:

- Backup full diário + backup de logs de bases de dados
- Período de retenção em disco por um período mínimo de 4 semanas para recuperações operacionais rápidas (tanto para o Datacenter Central como para as delegações)
- Considerar retenções em disco adicionais para longa retenção de 12 meses 3 anos respetivamente (a manter no Datacenter Central)
- Consideração de taxa de crescimento anual de 10% para um período de 3 anos

1.4 Capacidade de performance e escalabilidade necessárias para assegurar proteção de investimento e futuras necessidades:

- Capacidade de escrita correspondente a até pelo menos 9TB/hora
- Capacidade de expansão, sem recursos a troca de controlador de até pelo menos 90TB úteis, excluindo efeitos de deduplicação e/ou compressão;
- Suporte para protocolos NFS/CIFS e OpenStorage (e em simultâneo se necessário);

- Capacidade de backup direto para o repositório de dados, sem recurso a software de backup, para aplicações Oracle, SAP, SAP HANA e Microsoft SQL;

1.5 O repositório de proteção de dados deverá permitir a realização das diversas operações de backup, recuperação, replicação, sem necessidade de interrupção ou janela dedicada para as tarefas de manutenção do repositório;

1.6 A solução deverá fornecer e incluir todo o software necessário ao funcionamento da mesma, incluindo a capacidade de exportar dados para a cloud (pública e/ou privada);

1.7 A solução deverá ser fornecida sem limites de clientes e/ou agentes aplicacionais;

1.8 No sentido de garantir a mínima integridade dos dados armazenados, a solução deverá contemplar ao nível do repositório de dados os seguintes níveis mínimos de redundância e validação:

- Fontes de alimentação redundantes
- Proteção de disco de dupla paridade (RAID6)
- Mecanismo de verificação de integridade dos dados durante a escrita

1.9 A solução deverá ainda ser fornecida em formato PBBA (Purpose-Built Backup Appliance), ou seja, ter um conjunto de características diferenciadoras dos restantes dispositivos appliances e storage arrays tradicionais, onde se destaca:

- Serem capazes de armazenar especificamente dados de backup no formato do software de backup, sendo impraticável o uso dos dados para outros propósitos;
- Implementação de elevadas taxas de deduplicação (normalmente 10:1 ou mais), sendo impraticável o uso dos dados para outras tarefas que não recuperações;
- Permitir a replicação de dados em elevada eficiência (maioritariamente devido à deduplicação dos dados) por forma a facilitar backups rápidos a partir de localizações remotas;
- Fornecer tradução de protocolo (p.e. S3, OpenStack) para transferência de dados para repositórios de cloud (“cloud tiering”).

Nota: Os itens indicados neste ponto estão de acordo com os critérios considerados relevantes pela entidade independente Gartner Group.

Pretende-se que a tecnologia de ciberproteção implementada, suporte os seguintes conceitos, na sua implementação, operacionalidade e gestão:

1) Pretende-se proteger até 14 cópias da informação protegida no Datacenter Central (incluído a informação das delegações), em que pelo menos 50% serão “Gold”, saudáveis para recuperação a partir de um ciber-incidente;
2) Por forma a reduzir a superfície de ataque, a solução deverá recorrer a um isolamento lógico (do tipo air-gap) do cofre, desligado da rede face à produção, gerido a partir do próprio cofre e com acesso restrito apenas a utilizadores com as devidas credenciais de acesso ao cofre;

3) Transferência de dados protegida por handshake digital, encriptação do link de replicação e dos dados a sincronizar;
4) Proteger as cópias sincronizadas através de um mecanismo de retenção certificado, que garanta a imutabilidade dos dados protegidos no cofre;
5) Analítica integrada que permita a análise periódica dos dados contidos no formato nativo de backup, sem necessidade de "restores" e a procura de indicadores de comprometimento da informação;
6) A analítica deverá efetuar a análise dos dados com recurso a indexação total de conteúdos, dentro do cofre, sem qualquer recurso ou ligação ao exterior;
7) Gestão baseada em políticas e automatização dos workflows de proteção;
8) A solução a propor deverá incluir toda a infraestrutura necessária ao regular funcionamento do cofre, incluindo, mas não se limitando a: computação, armazenamento, ativos de rede e de segurança, todo o software e licenciamento necessário à análise dos dados a proteger no cofre.
9) A solução deverá ainda contemplar todos os serviços de implementação da solução de ciberproteção, bem como a realização de testes que permitam aferir o sucesso de implementação da mesma, de acordo com os requisitos a definir entre o IEFP e o proponente da solução

Cláusula 26.ª

Serviços de instalação, suporte e manutenção

1. O proponente deverá assegurar o suporte e manutenção de toda a solução fornecida, devendo o mesmo ser assegurado diretamente e por um único fabricante com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção pretendida é a seguinte:
2. Suporte e manutenção de 36 meses/3 anos com tempo de resposta de 4 horas, incluído peças e mão-de-obra.
   a) Prestação de assistência contínua até à solução da avaria.
   b) O suporte deverá ser dado diretamente pelo fabricante localmente (preferencialmente em língua portuguesa) sem recorrer a qualquer parceiro para esse efeito.
3. O proponente deverá ainda incluir todos os serviços necessários à instalação e configuração inicial do repositório de proteção de dados, bem como os serviços de interligação com a infraestrutura do IEFP.
4. Deverão ser propostos serviços para a realização de testes de backup e de recuperação, após a integração e a definir em conjunto com as equipas do IEFP.

Cláusula 27.ª

Penalidades

1. A penalidade por incumprimento do tempo de resposta definido n.º 2 da Cláusula anterior será aplicada consoante o que se encontra definido no nº 2 da presente Cláusula e será aplicada por cada ocorrência verificada.

2. O valor da penalidade é calculado por referência ao valor anual dos serviços de manutenção, correspondendo o montante dessa penalidade a 0,5% do mesmo.

3. As penalidades a aplicar nos termos dos números anteriores devem ser revertidas para a entidade adjudicante, sob a forma de nota de crédito, a qual se repercutirá na fatura correspondente à próxima anuidade, exceto se a penalidade se verificar no último ano do contrato. Neste caso, o valor da penalidade será revertido para a entidade adjudicante, no prazo máximo de 60 dias após a data em que foi exercido o referido direito, conforme estabelecido no nº 3 da cláusula anterior.