

CADERNO DE ENCARGOS

Aquisição Solução Backups & Disaster Recovery

Capítulo I – Disposições Gerais

Cláusula 1.ª

(Objeto)

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento de Consulta Prévia adotado para a formação do contrato de aquisição de bens móveis que tem por objeto principal a “Aquisição Solução Backups & Disaster Recovery”.

Cláusula 2.ª

(Local e Prazos)

1. Sem prejuízo das obrigações que devam perdurar para além da cessação do contrato, este mantém-se em vigor até à conclusão das prestações que fazem parte do mesmo, em conformidade com o previsto no Caderno de Encargos.
2. Os bens objeto do contrato devem ser entregues nas instalações da GO Porto, no prazo de 12 (doze) semanas a contar da data de outorga do contrato.
3. Os bens objeto do contrato devem ser montados, instalados e ensaiados, no local de entrega, no prazo de 15 (quinze) dias a contar da data de entrega.

Capítulo II – Obrigações Contratuais

Secção I - Obrigações do Fornecedor

Cláusula 3.ª

(Obrigações principais do Fornecedor)

Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, decorrem para o Fornecedor as seguintes obrigações principais:

- a) Obrigação de entrega dos bens, constantes no **Anexo I** do presente Caderno de Encargos;
- b) Obrigação de garantia dos bens.

Cláusula 4.ª

(Obrigações acessórias do Fornecedor)

Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, decorrem para o Fornecedor as seguintes obrigações acessórias:

- a) Transporte dos bens para o local de entrega;
- b) Montagem dos bens;
- c) Instalação dos bens;

d) Ensaio dos bens;

Cláusula 5.^a

(Conformidade e operacionalidade dos bens)

1. O Fornecedor obriga-se a entregar à Entidade Adjudicante os bens objeto do contrato com as características, especificações e requisitos técnicos previstos no Mapa de Quantidades, anexo ao presente Caderno de Encargos e que dele faz parte integrante.
2. Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.
3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens.
4. O Fornecedor é responsável perante a Entidade Adjudicante por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues, bem como durante o período de garantia.
5. Sem prejuízo do disposto especificamente no presente Caderno de Encargos e nos elementos que o integram, os bens a fornecer devem cumprir, nomeadamente, toda a legislação e normas relativas à proteção e segurança contra incêndios, proteção ambiental e segurança sísmica.

Cláusula 6.^a

(Entrega dos bens objeto do contrato)

O Fornecedor obriga-se a disponibilizar, simultaneamente com a entrega dos bens objeto do contrato e em língua portuguesa, todos os documentos que sejam necessários para a boa e integral utilização ou funcionamento daqueles.

Cláusula 7.^a

(Inspeção)

1. Após solicitação do Fornecedor, a Entidade Adjudicante, por si ou através de terceiro por ela designado, procede, no prazo de 15 (quinze) dias, à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar, respetivamente, se os mesmos correspondem às quantidades estabelecidas e se reúnem as características, especificações e requisitos técnicos e operacionais exigidas.
2. A inspeção qualitativa a que se refere o número pode ser realizada através de testes que a Entidade Adjudicante entenda realizar.
3. Durante a fase realização de testes o Fornecedor deve prestar à Entidade Adjudicante toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar durante a

realização daqueles, através de pessoas devidamente credenciadas para o efeito.

4. Os encargos com a realização dos testes, desde que devidamente comprovados, são da responsabilidade do Fornecedor.

Cláusula 8.^a

(Inoperacionalidade, defeitos ou discrepâncias)

1. No caso de não se verificar a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos exigidos, a Entidade Adjudicante deve informar, por escrito, o Fornecedor.
2. No caso previsto no número anterior, o Fornecedor deve proceder, à sua custa e no prazo que for determinado pela Entidade Adjudicante, às reparações ou substituições necessárias para garantir a operacionalidade dos bens e o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.
3. Após a realização das reparações ou substituições necessárias pelo Fornecedor, no respetivo prazo, a Entidade Adjudicante pode proceder à realização de novos testes, nos termos da Cláusula anterior.

Cláusula 9.^a

(Aceitação dos bens)

1. Deve ser emitido, no prazo máximo de 15 (quinze) dias, a contar da data em que se verifique a total operacionalidade dos bens objeto do contrato, de acordo com o previsto no Caderno de Encargos, um auto de receção assinado pelo representante da Entidade Adjudicante.
2. Com a assinatura do auto a que se refere o número anterior, ocorre a aceitação dos bens e a transferência da posse e da propriedade para a Entidade Adjudicante, bem como do risco de deterioração ou perecimento dos mesmos, sem prejuízo das obrigações de garantia que impendem sobre o Fornecedor.

Cláusula 10.^a

(Garantia)

1. O Fornecedor garante os bens objeto do contrato, pelo prazo mínimo de 2 (dois) anos a contar da data da assinatura do auto de receção, contra quaisquer defeitos ou discrepâncias com as exigências legais e com características, especificações e requisitos técnicos exigidos, que se revelem a partir da respetiva aceitação do bem.
2. A garantia prevista no número anterior abrange:
 - a) O fornecimento, a montagem ou a integração de quaisquer peças ou componentes em falta;

- b) A desmontagem de peças, componentes ou bens defeituosos ou discrepantes;
 - c) A reparação ou a substituição das peças, componentes ou bens defeituosos ou discrepantes;
 - d) O fornecimento, a montagem ou instalação das peças, componentes ou bens reparados ou substituídos;
 - e) O transporte do bem ou das peças ou componentes defeituosos ou discrepantes para o local da sua reparação ou substituição e a devolução daqueles bens ou a entrega das peças ou componentes em falta, reparados ou substituídos;
 - f) A deslocação ao local da instalação ou de entrega;
 - g) A mão-de-obra.
3. No prazo máximo de 2 (dois) meses a contar da data em que a Entidade Adjudicante tenha detetado qualquer defeito ou discrepância, esta deve notificar o Fornecedor, para efeitos da respetiva reparação ou substituição.
4. A reparação ou substituição devem ser realizadas dentro do prazo fixado pela Entidade Adjudicante e sem grave inconveniente para esta última, tendo em conta a natureza do bem e o fim a que o mesmo se destina.

Cláusula 11.^a

(Continuidade de fabrico)

O Fornecedor deve assegurar a continuidade do fabrico e do fornecimento de todas as peças, componentes e equipamentos que integram os bens objeto do contrato pelo prazo estimado de vida útil dos bens, de acordo com as regras de amortização contabilística aplicáveis.

Cláusula 12.^a

(Dever de sigilo)

1. O Fornecedor deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à Entidade Adjudicante, 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 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 13.^a

(Prazo do dever de sigilo)

O dever de sigilo mantém-se em vigor até ao termo do prazo de 4 (quatro) anos a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Secção II - Obrigações da Entidade Adjudicante

Cláusula 14.^a

(Preço)

1. O preço base do procedimento é de **51.675,39 € (cinquenta e um mil, seiscentos e setenta e cinco euros e trinta e nove cêntimos)**, significando este o preço máximo que a Entidade Adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o objeto do contrato a celebrar.
2. Pela execução de todas as prestações que constituem o objeto do contrato a celebrar, a Entidade Adjudicante pagará ao Fornecedor a quantia total indicada na sua proposta, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
3. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à Entidade Adjudicante, nomeadamente, os relativos ao transporte dos bens objeto do contrato para o respetivo local de entrega, montagem, instalação e ensaios, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 15.^a

(Condições de pagamento)

1. As quantias devidas pela Entidade Adjudicante devem ser pagas no prazo de 60 (sessenta) dias após a receção pela Entidade Adjudicante das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. Para os efeitos do número anterior, a obrigação considera-se vencida com a assinatura do auto de receção a que se refere o n.º 1 da Cláusula 9.^a.
3. Em caso de discordância por parte da Entidade Adjudicante, quanto aos valores indicados nas faturas, deve esta comunicar ao Fornecedor, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas são pagas através de transferência bancária.

Capítulo III – Penalidades contratuais e resolução

Cláusula 16.^a

(Penalidades contratuais)

1. Pelo incumprimento de obrigações emergentes do contrato, a Entidade Adjudicante pode exigir do Fornecedor o pagamento de penalidades contratuais, nos seguintes termos:
 - a) Pelo incumprimento das datas e prazos de entrega, instalação, montagem e ensaio dos bens objeto do contrato, 1‰ (um por mil) do preço contratual inicial, por cada dia de atraso;
 - b) Pelo incumprimento da obrigação de garantia técnica, 1‰ (um por mil) do preço contratual inicial, por cada dia de atraso na entrega dos bens reparados ou substituídos.
2. A Entidade Adjudicante pode compensar os pagamentos por si devidos com as penalidades devidas nos termos da presente Cláusula.
3. As penalidades previstas na presente Cláusula não obstam a que a Entidade Adjudicante exija uma indemnização pelo dano excedente.
4. A aplicação de qualquer sanção contratual pecuniária não desobriga o Fornecedor da sua obrigação principal, pelo que o cumprimento da mesma permanece exigível.

Cláusula 17.^a

(Força maior)

1. Não constituem causas de força maior, designadamente:
 - a) Greves ou conflitos laborais limitados às sociedades do Fornecedor ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - 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.
2. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
3. 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

(Resolução pela Entidade Adjudicante)

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, a Entidade Adjudicante pode resolver o contrato, a título sancionatório, no caso de o Fornecedor violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente, no caso de haver atraso, total ou parcial, na entrega dos bens objeto do contrato, na sua instalação, montagem ou ensaio, superior a 3 (três) meses ou declaração escrita do Fornecedor de que o atraso excederá esse prazo.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao Fornecedor e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pela Entidade Adjudicante.

Cláusula 19.ª

(Resolução 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 esteja em dívida há mais de 120 (cento e vinte) dias.
2. O direito de resolução é exercido por via judicial.
3. A resolução do contrato nos termos da presente Cláusula não determina a repetição das prestações já realizadas pelo Fornecedor, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444.º do CCP.

Capítulo IV – Caução e seguros

Cláusula 20.ª

(Caução)

1. Os termos da caução a prestar pelo Fornecedor são os previstos no Convite.
2. O Adjudicatário, no prazo de 10 (dez) dias úteis a contar da notificação de adjudicação, deve prestar caução, em valor correspondente a 5% (cinco por cento) do preço contratual, remetendo à Entidade Adjudicante, no dia imediatamente subsequente, o documento comprovativo de que a caução foi prestada.
3. No caso previsto no número anterior e, cumulativamente, quando o preço total resultante da proposta adjudicada seja considerado anormalmente baixo, por aplicação do disposto no n.º 1 do artigo 71.º do CCP, o Adjudicatário terá de prestar caução em valor correspondente a 10% (dez por cento) do preço contratual.
4. A caução prestada pelo Fornecedor representará, para todos os efeitos legais e contratuais, garantia de exato e pontual cumprimento do contrato e de todas as obrigações do Empreiteiro.

Cláusula 21.ª

(Execução da caução)

1. A caução prestada para bom e pontual cumprimento das obrigações decorrentes do contrato, referida na Cláusula anterior, pode ser executada pela Entidade Adjudicante, sem necessidade de prévia decisão judicial ou arbitral, para satisfação de quaisquer créditos resultantes de mora, cumprimento defeituoso e incumprimento definitivo pelo Fornecedor das obrigações contratuais ou legais, incluindo o pagamento de penalidades, ou para quaisquer outros efeitos especificamente previstos no contrato ou na lei.
2. A resolução do contrato pela Entidade Adjudicante não impede a execução da caução, contanto que para isso haja motivo.
3. A execução parcial ou total da caução referida nos números anteriores constitui o Fornecedor na obrigação de proceder à sua reposição pelo valor existente antes dessa mesma execução, no prazo de 8 (oito) dias após a notificação da Entidade Adjudicante para esse efeito.

Capítulo V – Disposições Finais

Cláusula 22.ª

(Subcontratação)

1. O Fornecedor pode subcontratar desde que se encontrem cumpridos os requisitos constantes dos n.ºs 3 e 6 do artigo 318.º do CCP.
2. A Entidade Adjudicante pode opor-se à subcontratação na fase de execução do contrato quando não estejam verificados os limites constantes do artigo 317.º do CCP, ou quando haja fundado receio de que a subcontratação envolva um aumento de risco de incumprimento das obrigações emergentes do contrato.
3. Todos os subcontratos devem conter uma cláusula na qual o Subcontratado declara que conhece, integralmente, o presente Caderno de Encargos, nomeadamente, as cláusulas referentes à subcontratação e ao pagamento direto aos Subcontratados.
4. Todos os subcontratos devem ter em anexo o mapa de trabalhos e quantidades de que será objeto a subcontratação, tendo por base o mapa de trabalhos e quantidades do presente procedimento, fazendo coincidir, sem exceção, a numeração dos artigos e a correspondente descrição.
5. O disposto nos números anteriores é igualmente aplicável aos contratos celebrados entre os Subcontratados e terceiros.
6. No prazo de 5 (cinco) dias após a celebração de cada subcontrato, o Fornecedor deve comunicar por escrito o facto à Entidade Adjudicante, remetendo-lhe cópia do contrato em causa.
7. A responsabilidade pelo exato e pontual cumprimento de todas as obrigações contratuais é do Fornecedor, ainda que as mesmas sejam cumpridas por recurso a Subcontratados.

8. O incumprimento do previsto nos n.ºs 3 e 4 da presente Cláusula, é considerado uma violação grave do contrato, podendo a Entidade Adjudicante aplicar ao Fornecedor, uma sanção contratual, no valor de **5.000,00 € (cinco mil euros)**, por cada violação.
9. É lícito ao Fornecedor recorrer a auxiliares que a coadjuvem no cumprimento da sua prestação contratual sem, todavia, nunca o substituírem.

Cláusula 23.ª

(Pagamentos diretos a Subcontratados)

1. O Subcontratado pode reclamar, junto da Entidade Adjudicante, os pagamentos em atraso que lhe sejam devidos pelo Fornecedor.
2. No caso previsto no número anterior a Entidade Adjudicante notifica o Fornecedor para, no prazo de 10 (dez) dias:
 - a) Efetuar o pagamento; ou
 - b) Opor-se ao pagamento, apresentando motivo justificativo, devendo, quando aplicável, indicar o prazo, não superior a 30 (trinta) dias, no qual se propõe efetuar o pagamento em atraso.
3. O Fornecedor deve, em qualquer dos casos de pagamento referidos nas alíneas do número anterior e dentro do prazo que delas decorra, enviar à Entidade Adjudicante comunicação a informar que o pagamento foi efetuado.
4. A Entidade Adjudicante apenas procederá ao pagamento direto ao Subcontratado se:
 - a) O quadro normativo especificamente aplicável à execução do contrato não proibir a realização de pagamentos a terceiros;
 - b) O Fornecedor não se opuser, injustificadamente, ao pagamento ao Subcontratado;
 - c) O Fornecedor, no prazo fixado no n.º 3, não proceder ao envio para a Entidade Adjudicante da comunicação aí prevista.
5. No caso de o Subcontratado interpelar a Entidade Adjudicante, nos termos e para os efeitos da presente Cláusula, este apenas procederá ao pagamento ao Fornecedor quando tiver sido concluído o procedimento previsto nos n.ºs 2, 3 e 4 da presente Cláusula, nomeadamente e quando aplicável, após o envio da comunicação a informar que o pagamento foi efetuado.
6. É aplicável o previsto nos n.ºs 4 e 5 do artigo 321.º-A do CCP.

Cláusula 24.ª

(Cessão da posição contratual)

1. É admitida a cessão da posição contratual por qualquer das partes, dependendo, no caso da cessão da posição contratual por parte do Fornecedor, da autorização prévia da Entidade Adjudicante e do cumprimento do previsto nos artigos 316.º a 324.º do CCP.
2. Em caso de incumprimento, pelo Fornecedor, das suas obrigações, que reúna os pressupostos

para a resolução do contrato, a Entidade Adjudicante pode fazer uso do mecanismo previsto no artigo 318.º-A do CCP, cedendo o Fornecedor a sua posição contratual nos termos aí previstos.

Cláusula 25.ª

(Cessão de créditos)

1. O Fornecedor não pode ceder ou dar como garantia o contrato de fornecimento ou qualquer dos direitos ou obrigações nele estipulados, designadamente, totalidade ou parte dos créditos emergentes do contrato sem prévio acordo escrito da Entidade Adjudicante, nos termos do disposto nos artigos 577.º e seguintes do Código Civil.
2. Em caso de incumprimento do previsto na presente Cláusula, além de ser considerada uma violação grave do contrato, a Entidade Adjudicante pode aplicar ao Fornecedor, uma sanção contratual, no valor de **5.000,00 € (cinco mil euros)**, por cada violação, isto é, por cada cessão de créditos efetuada

Cláusula 26.ª

(Modificações objetivas do contrato)

Sem prejuízo das modificações objetivas prevista no presente Caderno de Encargos e no artigo 447.º-A do CCP, são admitidas as seguintes modificações objetivas:

- a) Prorrogação do prazo para execução do fornecimento, por causas imputáveis à Entidade Adjudicante;
- b) Prorrogação do prazo da execução do fornecimento, por causas de força maior.

Cláusula 27.ª

(Proteção de dados)

1. O Fornecedor 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 (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD).
2. O Contraente Público, no caso de suspeitar da verificação de algum incumprimento do RGPD, deve notificar o Fornecedor para este, no prazo de 5 (cinco) dias, demonstrar o total cumprimento do referido regulamento.
3. Caso o Fornecedor não demonstre o total cumprimento do RGPD, seja porque não o demonstrou, seja porque não o cumpre, o Contraente Público fica autorizado a proceder à auditoria aos sistemas de informação do Fornecedor, ficando este responsável por todos os custos dessa auditoria.
4. No caso previsto no número anterior, o Contraente Público poderá compensar os custos que tenha suportado com eventuais quantias que sejam devidas ao Fornecedor, ou através do acionamento da caução, caso esta tenha sido prestada, ou através do recurso às retenções que

- eventualmente tenham sido efetuadas.
5. No caso de se verificar algum incumprimento do RGPD por parte do Fornecedor, este deverá, no prazo de 10 (dez) dias, pôr fim ao incumprimento e demonstrá-lo ao Contraente Público.
 6. O não cumprimento do RGPD é considerado, para todos os efeitos, um incumprimento muito grave do contrato, podendo o Contraente Público resolver o contrato.
 7. Caso o Fornecedor impeça ou não colabore na realização da auditoria referida no n.º 3 da presente Cláusula, o Contraente Público poderá resolver o contrato, por incumprimento muito grave do Fornecedor.

Cláusula 28.ª

(Avaliação do Fornecedor)

A prestação contratual do Fornecedor será avaliada em conformidade com os critérios específicos definidos pela Entidade Adjudicante para o efeito, critérios esses que se encontram disponíveis no website da GO Porto, em cumprimento do disposto na norma NP EN ISO 9001:2015.

Cláusula 29.ª

(Foro competente)

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal do Porto, com expressa renúncia a qualquer outro.

Cláusula 30.ª

(Legislação aplicável)

Em tudo o omissso no presente Caderno de Encargos, observar-se-á o regime do CCP e restante legislação aplicável.

Cláusula 31.ª

(Contagem dos prazos)

Os prazos previstos são contínuos, não se suspendendo nos sábados, domingos e dias feriados.

ANEXO I

• **Servidor VSA:**

1 (um) servidor com as seguintes características mínimas:

a) 2 (dois) CPU's de última geração, cada um com:

- 8-Cores (oito cores);
- Velocidade de relógio de 2.8Ghz (dois vírgula oito Gigahertz);
- Consumo máximo de 105 Watts (cento e cinco watts);

b) Altura máxima em bastidor: 2U (doisU)

c) 64GB (sessenta e quatro Gigabytes) de memória RAM, com capacidade de expansão a 8TB (oito Terabytes) distribuídos por 32 (trinta e duas) slots DIMM;

d) Deverá apresentar escalabilidade interna para um mínimo de 12 (doze) discos, dentro do mesmo chassis, os quais deverão ter um indicador de utilização (para evitar perda de dados ou downtime, devido a remoção indevida de discos);

e) Um mínimo de 1 (uma) controladora de discos com capacidade para RAID 0 (zero), 1 (um), 5 (cinco), e RAID 10 (dez), com mínimo de 4GB (quatro Gigabytes) de cache protegida por bateria;

f) 2 (dois) discos SSD com mínimo de 480GB (quatrocentos e oitenta Gigabytes);

g) 8 (oito) discos SAS 12G de 7.2K LFF de 2TB (dois Terabytes);

h) 5 (cinco) Portas USB 3.0 (três ponto zero) distribuídas pela dianteira, traseira e interior do servidor;

i) 2 (duas) portas ethernet a 10Gb/s (dez Gigabits por segundo) com interface do tipo SFP+ e respetivos transceivers 10Gb (dez Gigabits) SFP+ SR;

j) 4 (quatro) portas ethernet a 1Gb/s (um Gigabit por segundo) com interface do tipo RJ45. Estas portas deverão ser disponibilizadas sem consumo de qualquer slot PCI;;

k) 1 (uma) porta ethernet 1Gb/s (um Gigabit por segundo) dedicada a gestão remota avançada;

l) O servidor proposto deverá ser suportado para utilização em Rack. Deverá suportar a instalação de calhas adequadas para o efeito;

m) Deverá incluir duas fontes de alimentação redundantes e Hot-Plug de no mínimo 800W Platinum;

n) A porta dedicada a Gestão remota, deverá incluir consola gráfica remota, e pelo menos as seguintes funcionalidades:

- Consola gráfica;
- Controlo energético;

- Atualizações de firmware;
 - configurações na Bios;
 - virtual media de modo unificado.
- o) O servidor a propor deverá incluir capacidade de comunicação com plataforma de monitorização em cloud disponibilizada pelo fabricante que inclua tecnologia de inteligência artificial para análise e tratamento de eventos relacionados com suporte preditivo e mitigação de risco. Todo o licenciamento, caso exista, deve estar incluído para a totalidade da solução. Este sistema deverá pelo menos disponibilizar a seguinte informação:
- Inventário global de servidores;
 - Vista consolidada com o estado geral e conectividade dos servidores;
 - Capacidade de aprendizagem global com deteção preditiva de eventuais problemas;
 - Relatório global de garantia e suporte, assim como idade de cada servidor;
 - Inventário detalhado do servidor (Hardware, Firmware e Software, Drivers, logs e eventos) com a possibilidade de extrair relatórios;
 - Histórico de casos de suporte com a opção de criação de casos novos;
 - Coleta Automática de dados de telemetria e sensores usando (0) zero recursos dos servidores;
 - Análise preditiva de falhas de peças dos servidores;
 - Análise de problemas de firmware, driver, SO / hypervisor e software do sistema;
 - Notificações de alertas por email;
 - Recomendações e aconselhamento para o bom funcionamento do servidor.
- p) O servidor a propor deverá permitir a configuração de mecanismo de abertura automática de chamadas de suporte em caso de falha ou pré-falha do tipo “call home”.

Serviços de suporte

- Os serviços de Manutenção de hardware e software deverão ser prestados para uma duração de 3 (três) anos, com uma cobertura 9x5 (nove horas, cinco dias por semana) e com resposta no dia útil seguinte, assegurando abertura de chamada automática via ligação segura https;
- A manutenção deverá ser assegurada pelo fabricante dos equipamentos;
- A reparação de Hardware deverá apenas ser realizada com peças genuínas do fabricante dos equipamentos;
- Deve ser implementada uma solução de suporte para permitir a abertura automática de chamadas, no caso de incidentes de falha ou pré-falha de algum componente.

- **Servidor Disaster & Recovery:**

1 (um) servidor com as seguintes características mínimas:

a) 2 (dois) CPU's de última geração, cada um com:

- 8-Cores (oito Cores);
- Velocidade de relógio de 2.8Ghz (dois vírgula oito Gigahertz);
- Consumo máximo de 105 Watts (cento e cinco Watts);

b) Altura máxima em bastidor: 2U (dois U);

c) Licenciamento Windows Server 2019 necessário para a solução proposta;

d) 128GB (cento e vinte e oito Gigabytes) de memória RAM, com capacidade de expansão a 8TB (oito Terabytes) distribuídos por 32 (trinta e duas) slots DIMM;

e) Deverá apresentar escalabilidade interna para um mínimo de 8 (oito) discos, dentro do mesmo chassis, os quais deverão ter um indicador de utilização (para evitar perda de dados ou downtime, devido a remoção indevida de discos);

f) Um mínimo de 1 (uma) controladora de discos com capacidade para RAID 0 (zero), 1 (um), 5 (cinco), e RAID 10 (dez), com mínimo de 2GB (dois Gigabytes) de cache protegida por bateria;

g) 2 (dois) discos SSD com mínimo de 240GB (duzentos e quarenta Gigabytes);

h) 6 (seis) discos SSD com mínimo de 3.84TB (três vírgula oitenta e quatro Terabytes);

i) 5 (cinco) Portas USB 3.0 (três ponto zero) distribuídas pela dianteira, traseira e interior do servidor;

j) 4 (quatro) portas ethernet a 1Gb/s (um Gigabit por segundo) com interface do tipo RJ45 - Estas portas deverão ser disponibilizadas sem consumo de qualquer slot PCI;

k) 4 (quatro) portas ethernet a 1Gb/s (um Gigabit por segundo) com interface do tipo RJ45;

l) 1 (uma) porta ethernet 1Gb/s (um Gigabit por segundo) dedicada a gestão remota avançada;

m) O servidor proposto deverá ser suportado para utilização em Rack. Deverá suportar a instalação de calhas adequadas para o efeito;

n) Deverá incluir duas fontes de alimentação redundantes e Hot-Plug de no mínimo 800W (oitocentos Watts) Platinum;

o) A porta dedicada a Gestão remota, deverá incluir consola gráfica remota, e pelo menos as seguintes funcionalidades:

- Consola gráfica;
- Controlo energético;
- Atualizações de firmware;
- configurações na Bios;

- virtual media de modo unificado.

p) O servidor a propor deverá incluir capacidade de comunicação com plataforma de monitorização em cloud disponibilizada pelo fabricante que inclua tecnologia de inteligência artificial para análise e tratamento de eventos relacionados com suporte preditivo e mitigação de risco. Todo o licenciamento, caso exista, deve estar incluído para a totalidade da solução. Este sistema deverá pelo menos disponibilizar a seguinte informação:

- Inventário global de servidores;
- Vista consolidada com o estado geral e conectividade dos servidores;
- Capacidade de aprendizagem global com deteção preditiva de eventuais problemas;
- Relatório global de garantia e suporte, assim como idade de cada servidor;
- Inventário detalhado do servidor (Hardware, Firmware e Software, Drivers, logs e eventos) com a possibilidade de extrair relatórios;
- Histórico de casos de suporte com a opção de criação de casos novos;
- Coleta Automática de dados de telemetria e sensores usando (0) zero recursos dos servidores;
- Análise preditiva de falhas de peças dos servidores;
- Análise de problemas de firmware, driver, SO / hypervisor e software do sistema;
- Notificações de alertas por email;
- Recomendações e aconselhamento para o bom funcionamento do servidor.

q) O servidor a propor deverá permitir a configuração de mecanismo de abertura automática de chamadas de suporte em caso de falha ou pré-falha do tipo “call home”

Serviços de suporte

- Os serviços de Manutenção de hardware e software deverão ser prestados para uma duração de 3 (três) anos, com uma cobertura 9x5 (nove horas, cinco dias por semana) e com resposta no dia útil seguinte, assegurando abertura de chamada automática via ligação segura https;
- A manutenção deverá ser assegurada pelo fabricante dos equipamentos;
- A reparação de Hardware deverá apenas ser realizada com peças genuínas do fabricante dos equipamentos;
- Deve ser implementada uma solução de suporte para permitir a abertura automática de chamadas, no caso de incidentes de falha ou pré-falha de algum componente.

- **Solução de Backups para disco**

- a) A solução de backup baseada em disco proposta deve ser um verdadeiro / puro aplicativo de proteção de dados definido por software (sendo chamado de aplicativo virtual) e estará disponível em plataformas virtualizadas como VMware, Hyper-V etc;
- b) O aplicativo virtual proposto será qualificado para trabalhar em servidores de fornecedores de renome cumprindo os padrões da indústria;
- c) O aplicativo virtual proposto deve ser oferecido com um mínimo de 14TB (catorze Terabytes) de capacidade utilizável;
- d) O aplicativo virtual proposto deve ser eficiente em recursos e não consumir mais de 100MB (cem Megabytes) de memória virtual por TB e mais em ambiente virtualizado;
- e) O aplicativo virtual proposto deve ser qualificado para trabalhar tanto com Ethernet como com conectividade Fiber Channel para o hospedeiro conectado. O fornecedor deve fornecer o número necessário de Fiber Channels e portas Ethernet de acordo com o requisito de solução;
- f) O aplicativo virtual proposto deve ser certificado para trabalhar com pelo menos 3 fornecedores de aplicações de backup ISV como HPE, Veritas, Dell-EMC, Veeam, Commvault, etc;
- g) O aplicativo virtual proposto deve ser escalável para pelo menos 500TB (quinhentos Terabytes) utilizáveis em modo nativo (sem de-duplicação e compressão) e 1PB (um Petabyte) adicional de capacidade utilizável nativa utilizando armazenamento na nuvem como AWS, Azure ou em armazenamento de objetos;
- h) O fornecedor não deve utilizar nenhum dispositivo adicional de “staging” enquanto desloca os dados do aplicativo Virtual para a nuvem pública ou o armazenamento de objetos;
- i) O aplicativo virtual proposto deve suportar a emulação do alvo VTL e NAS como o CIFS;
- j) O aplicativo virtual proposto terá a capacidade de fazer cópia completa de conjuntos de dados a partir do armazenamento de backup em disco para o armazenamento em nuvem, em vez de tiering de dados;
- k) O aplicativo virtual proposto terá a capacidade de configurar pelo menos uma combinação de 32 (trinta e duas) tape libraries e objetos NAS, juntamente com 32.000 (trinta e duas mil) ou mais Cartridge slots, ao escalar para a máxima capacidade utilizável;
- l) O aplicativo virtual proposto terá a capacidade de fornecer restauro seletivo do próprio aplicativo virtual;
- m) O aplicativo virtual proposto deve integrar e utilizar a atual infraestrutura de backup em Tape do cliente nos seguintes aspetos:
 - Compatibilidade com os servidores de backup / media servers existentes no cliente;
 - Compatibilidade com tape library e tape drives;

- Compatibilidade com o software de backup existente.
- n) O aplicativo virtual proposto deve ter licença integrada de deduplicação, licença de replicação de baixa largura de banda para que apenas transferências de blocos não duplicados únicas para localização remota/DR;
- o) A replicação para o site DR deve ser qualificada de forma nativa quer em aplicativo virtual quer em aplicativo físico do mesmo fornecedor;
- p) O dispositivo proposto deve ter informações para compreender a deduplicação source based e target based e deve ser integrado com todos os ISVs de backup reconhecidos, como Veritas, Commvault e Veeam, etc. Devem ser apoiados pelo menos 3 (três) ISV;
- q) Capacidade de emular flexivelmente tape drives/formatos LTO-Gen5, LTO-Gen6 e LTO-Gen7 etc;
- r) As portas de Fiber channel devem suportar conectividade de servidores de forma direta ou via switches SAN enquanto suportam tanto a de-duplicação source e target based;
- s) O dispositivo de backup baseado em disco proposto também deve suportar a funcionalidade de encriptação.

- **Software Backups:**

A solução deve ser capaz de fornecer proteção total da infraestrutura virtual incluindo capacidades de Disaster Recovery e continuidade do negócio, para uma quantidade de 10 (dez) máquinas virtuais.

A solução deve respeitar os requisitos mínimos que se descrevem de seguida.

Requisitos Mínimos:

- A solução de Backup deve funcionar com a infraestrutura VMware baseada nas versões 5.5, 6.X, 7.0 (até U2) e VMware Cloud on AWS e / ou Microsoft Hyper-V 2008 R2 SP1, Hyper-V 2012, Hyper-V 2012 R2, Hyper-V 2016, Hyper-V 2019, and Hyper-V 2022 e / ou Nutanix Acropolis;
- A solução deve suportar hosts geridos pelo VMware vCenter Server e também standalone hosts;
- A solução deve suportar vCloud Director for VMware;
- A solução deve suportar Hyper-V hosts manager by System Center Virtual Machine Manager (2012 SP1 and R2, 2016, 1801, 1807, e 2019), clustered hosts e standalone hosts;
- A solução deve suportar a cópia de segurança de todos os sistemas operativos suportados pelo VMware, Hyper-V ou Acrópolis;
- A solução deve incorporar imagens de cópias de segurança das Máquinas Virtuais e replicação das Máquinas Virtuais baseadas no host para o site de Disaster Recovery geridas por uma única consola sem custo extra;
- A solução deve integrar com Object Storage (pelo menos S3, S3-like e Blob storage) sem custo extra;
- A solução deve permitir automação através de uma RESTFUL API ou um PowerShell SDK;
- A solução deve permitir partilhas de ficheiros NAS, independentemente do tipo de NAS (SMB -versão 1,2, ou 3, NFS- versão 3, ou 4.1- ou servidores de partilha de ficheiros Windows-ou Linux;
- Licenciamento necessário para a solução proposta.

Arquitetura:

- A solução deve ser agentless e deve ser capaz de efetuar cópia de segurança de Servidores Virtuais incluindo SO e Aplicações, para ambientes virtuais que executem VMware, Hyper-V e / ou AHV, e para os três maiores hyperscalers (AWS, Microsoft Azure, GCP);

- A solução deve fornecer agentes O.S para servidores físicos. Estes agentes devem garantir consistência aplicacional com qualquer outro agente;
- A solução deve suportar arquitetura Disk-To-Disk-To-Tape D2D2T;
- A solução deve suportar qualquer tipo de armazenamento baseado em Disco (DAS/NAS/SAN);
- A solução deve fornecer um formato de ficheiro de backup self-sufficient para evitar o risco de perda de catálogo;
- A solução deve ser escalável, fornecendo uma forma fácil e de custo eficiente para manter o crescimento da infraestrutura sem afetar as janelas de backup;
- A solução deve suportar várias consolas de backup e fornecer um ponto central de gestão destas consolas;
- A solução deve suportar Object Storage para tecnologias de hardware como Azure Blob, AWS S3 e S3-like;
- A solução deve suportar Repositórios Imutáveis.

Proteção de Perda de Dados:

- A solução deve cumprir um objetivo de ponto de restauração de no mínimo 15 (quinze) minutos;
- A solução deve usar o VMware vStorage API for Data Protection e aproveitar o Change Block Tracking;
- A solução deve ser capaz de fazer backup automático de todas as configurações e fornecer recursos de restauro fáceis para a infraestrutura de backup em caso de falha;
- A solução deve fornecer backups sem dependências externas. Os arquivos de backup devem ser independentes;
- A solução deve ser capaz de fornecer um mecanismo de rastreamento de bloco de alterações para permitir backups incrementais mais rápidos;
- A solução deve suportar várias opções de modo de backup, incluindo SAN direta, LAN direta ou HOTADD;
- A solução deve suportar processamento paralelo de backup de VMs para reduzir a janela de backup;
- A solução deve permitir a execução de scripts pré e pós backup;
- A solução deve suportar os modos de backup incremental reverso, direto e contínuo com suporte para Full Synthetic para reduzir o impacto na infraestrutura de produção.
- A solução deve ser capaz de realizar backups de nível de imagem com

reconhecimento de aplicativo sem agente, incluindo integração total com o Microsoft VSS e a capacidade de truncar logs de transações do Exchange, SQL e/ou Oracle para ambientes VMware e Hyper-V;

- A solução deve fornecer integração nativa Oracle RMAN, certificada pela Oracle;
- A solução deve fornecer integração nativa SAP HANA, certificada SAP HANA;
- A solução deve fornecer recursos integrados de deduplicação, compactação e exclusão de troca para reduzir o tamanho dos requisitos de armazenamento de backup e economizar custos;
- A solução deve fornecer um mecanismo de controle de E/S de backup integrado para evitar alta latência de armazenamento durante o backup. A solução deve fornecer controle de latência globalmente e por armazenamento de dados individual;
- A solução deve ser capaz de detetar instantâneos órfãos e consolidá-los adequadamente;
- A solução deve fornecer integração avançada com armazenamento SAN para realizar backups e replicações diretamente do Storage Snapshot para aumentar os RPOs e reduzir o impacto na produção;
- A solução deve ser capaz de criar uma cópia de todas ou de VMs selecionadas para um armazenamento de backup secundário no local ou externo automaticamente com a possibilidade de validação e correção;
- Tanto o Backup quanto a Cópia de Backup devem oferecer suporte às políticas de retenção GFS;
- A solução deve fornecer criptografia de ponta a ponta para arquivos de backup em diferentes mídias e comunicações de rede associadas usando criptografia AES 256 com Impacto Zero na velocidade das operações de backup;
- A solução deve fornecer um mecanismo que possa recuperar senhas de backup perdidas;
- A solução deve suportar arquivamento de backups de arquivos e VMs em fita. Bibliotecas independentes, Rotating Drives e VTLs devem ser suportadas;
- A solução deve fornecer backups de arquivamento para plataformas de nuvem pública, privada e híbrida;
- A solução deve fornecer mecanismo de Failover de VM Inteligente que inclui Re-IP automatizado e mapeamento de rede de VMs no local de DR e uma tecnologia de failback que transfere apenas blocos alterados de volta ao local de produção;
- A solução deve oferecer suporte à replicação de arquivos de backup para evitar sobrecarga na produção;

- A solução deve incluir orquestração de failover, permitindo um 1-click failover para evitar longos períodos de inatividade e fornecer quase alta disponibilidade;
- A solução deve oferecer uma função de aceleração de WAN integrada para permitir uma replicação mais rápida de cópia de backups de VM e Replicação de Host com suporte para links de WAN de baixa largura de banda e alta latência.

Recuperação:

- A solução deve estar em conformidade com o RTO Objetivo de Tempo de Restauração máximo de 15 (quinze) minutos;
- A solução deve ser capaz de restaurar instantaneamente qualquer máquina (uma ou mais) de qualquer tamanho diretamente de qualquer backup de qualquer ponto de restauração disponível no backup baseado em disco para VMware, Hyper-V e/ou Nutanix AHV, independentemente do tipo de backup (carga de trabalho virtual, física, na nuvem);
- A solução deve ser capaz de restaurar qualquer máquina (uma ou mais) de qualquer tamanho de qualquer backup diretamente para Amazon AWS, Microsoft Azure ou GCP;
- A solução deve habilitar a possibilidade de executar uma verificação antivírus antes de recuperar a máquina;
- A solução deve oferecer suporte à reversão rápida de VM usando CBT e restauração por SAN;
- A solução deve suportar configuração de VM e restauro de disco rígido virtual;
- A solução deve fornecer uma maneira fácil de restaurar o arquivo do sistema operativo convidado, incluindo, entre outros, Windows, Linux, Unix e BSD;
- A solução deve fornecer recursos de restauro granular diretamente do backup para todos os aplicativos virtualizados sem a necessidade de realizar backups adicionais baseados em agente. Essa funcionalidade deve incluir Active Directory, MS SQL, Oracle, MS Exchange e MS SharePoint;
- A solução deve aproveitar os snapshots de armazenamento para executar operações de restauro, incluindo restauro instantâneo de VM e restauro granular de arquivos e aplicativos sem a necessidade de hardware ou software adicional;
- A solução deve fornecer uma interface Web que permita aos operadores restaurar VMs completas, arquivos, itens de troca ou bases de dados SQL diretamente do backup;
- A solução deve ter um mecanismo de auto-atendimento que permita a delegação para proprietários de aplicativos restaurarem seus próprios arquivos e VMs.

Conformidade:

- A solução deve fornecer teste e verificação automatizados de cada backup ou réplica para garantir a capacidade de recuperação em caso de falha de produção. A verificação deve incluir arquivos de VM, sistema operativo e aplicativos, incluindo testes personalizados usando scripts;
- A solução deve fornecer acesso API aos dados de backup para executar verificações de segurança (ou seja, verificação antivírus), big data, mineração de dados, etc, sem recuperar nenhum dado;
- A solução deve ser capaz de criar ambientes de teste executando uma ou mais VMs diretamente de backup ou réplicas dentro de um ambiente isolado para uso de teste, desenvolvimento ou treinamento sem a necessidade de investir em computação ou armazenamento adicional;
- A solução deve ser capaz de verificar se um backup de VM está livre de vírus antes de restaurá-lo no ambiente de produção;
- A solução deve ser capaz de preparar e executar scripts de limpeza em conformidade com GDPR em uma VM antes de restaurá-la em um ambiente de produção.

Visibilidade:

- A solução deve fornecer monitoramento avançado, relatórios e planeamento de capacidade para a infraestrutura virtual e de backup;
- A solução deve ser capaz de fornecer monitorização de desempenho em tempo real 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, coletando dados num intervalo que inclua todas as principais métricas de desempenho, incluindo computação (CPU e RAM), armazenamento e rede;
- A solução deve permitir visualizar e analisar dados históricos de desempenho para entender as tendências e facilitar a solução de problemas;
- A solução deve fornecer recursos avançados para monitorar o desempenho e o status das tarefas de backup, relatar VMs protegidas e desprotegidas, descobrir e monitorar a prontidão do backup e os requisitos do repositório;
- A solução deve ser capaz de analisar uma configuração de VMs e mostrar possíveis problemas e possíveis limitações que podem ser atendidas durante o processo de backup (somente VMware);
- A solução deve ser capaz de enviar notificações de alarmes via e-mail personalizável e/ou protocolo SNMP;

- A solução deve garantir a cobertura completa da monitorização criando alarmes personalizados para eventos exclusivos do ambiente virtual;
- A solução deve ser capaz de realizar a modelagem de um alarme em relação a dados de desempenho anteriores para entender a frequência potencial de alarme e evitar problemas como tempestades de alertas inadvertidas e eventos perdidos;
- A solução deve permitir visualizar e gerenciar processos executados em servidores, hosts e VMs;
- A solução deve permitir personalizar e guardar modelos de relatórios para criar relatórios que atendam a informações específicas e necessidades de formatação;
- A solução deve ser capaz de ajudar a gerenciar o crescimento da infraestrutura virtual com recursos como análise de tendências, previsões de limites e recomendações de provisionamento;
- A solução deve ser capaz de criar diagramas do Visio que documentem a infraestrutura virtual;
- A solução deve ser capaz de descobrir VMs com recursos de memória e CPU sub e superutilizados e enviar recomendações sobre alocações adequadas de vCPU e vRAM;
- A solução deve ser capaz de gerar relatórios que rastreiem as alterações de configuração na infraestrutura virtual e de backup, incluindo o local da alteração e o utilizador autenticado para realizá-la.

- **1/8 G2 Autoloader - FC**

Fornecimento de um robot de tapes com as seguintes características:

- Suporte para drives LTO6 a LTO9;
- Capacidade de monitorização via web browser;
- Deve ser fornecido com uma drive LTO-8;
- Mínimo de 8 slots para tapes;
- Mínimo de 8 tapes LTO-8 com capacidade de leitura e escrita;
- Uma tape de limpeza;
- Dois cabos de fibra para ligação à SAN existente do tipo LC/LC com mínimo de 5 (cinco) metros;
- A drive LTO-8 proposta deve utilizar mecanismos de gestão de “buffers” de modo a fazer coincidir a velocidade da tape com a velocidade de transferência de dados para optimização do processo de escrita;
- A drive LTO-8 proposta tem que suportar tapes do tipo WORM além de suporte para encriptação AES 256 bit;
- A drive LTO-8 tem que suportar uma velocidade base de 300MB/sec (trezentos Megabytes por segundo);
- Deverá ainda a drive proposta suportar a utilização de tapes LTO-7 (Type M) para leitura e escrita;
- As ligações FC (Fibre channel) da tape têm que ser no mínimo a 8Gbps (oito Gigabits por Segundo).

- **Acessórios**

- 34 (trinta e quatro) chicotes UTP CAT6 3 (três) metros cinzento;
- 20 (vinte) chicotes UTP CAT6 2 (dois) metros cinzento;
- 2 (dois) cabos alimentação C13/C14 1,8 (um vírgula oito) metros;
- 12 (doze) discos para MSA 1.2TB 12G SAS 10K SFF (2.5in) Dual Port Enterprise 3yr Warranty Hard Drive;
- 1 (um) 16Gb (dezassexes Gigabits) Dual Port Fibre Channel Host Bus Adapter.