NAZARÉ

MUNICIPIO DA NAZARÉ
Câmara Municipal

INFORMAÇÃO

ASSUNTO: Aquisição de Bens – Servidor Informático (Datacenter)	**INFORMAÇÃO N.º:** 411/DAF-SAC/2023
	NIPG: 7685/23
	DATA: 2023/05/11
	REQUERIMENTO:

DELIBERAÇÃO:
Deliberado em reunião de câmara realizada em ...../...../.....,

O PRESIDENTE DA CÂMARA MUNICIPAL

Walter Manuel Cavaleiro Chicharro, Dr.

DESPACHO:

À Reunião
11-05-2023

Walter Manuel Cavaleiro Chicharro, Dr.
Presidente da Câmara Municipal da Nazaré

À Dra. Paula Veloso
Para inserir na "ordem do dia" da próxima reunião da Câmara Municipal, conforme Despacho do Sr. Presidente.
11-05-2023

Helena Pola
Chefe da Divisão Administrativa e Financeira

CHEFE DE DIVISÃO:

Exmo. Sr. Presidente da Câmara Municipal

Concordo com o exposto.
À consideração superior,
11-05-2023

Helena Pola
Chefe da Divisão Administrativa e Financeira

NAZARÉ

MUNICÍPIO DA NAZARÉ
Câmara Municipal

INFORMAÇÃO

APROVISIONAMENTO	CABIMENTO	DESPACHO COMPROMETA-SE	COMPROMISSO	N.º INTERNO	DESPACHO AUTORIZADO

Exma. Senhora Chefe, de Divisão Administrativa Financeira,

Considerando o cumprimento de instruções superiores;

Considerando que o Município da Nazaré tem a necessidade de renovar os componentes do servidor informático (*Datacenter),* pois, os que se encontram ao serviço, estão desatualizados e obsoletos.

Considerando a solicitação enviada pelo Eng. Tiago Santos, que se anexa, torna-se necessário proceder à aquisição de bens acima referida, pelo que se submete à apreciação da Exma. Câmara, em cumprimento da alínea b) do n.º 1 do artigo 20.º do Código dos Contratos Públicos, autorização para a realização do procedimento contratual de ***Concurso Público***.

Para o efeito, junto se anexam as peças do procedimento do Concurso, também para aprovação.

O prazo de fornecimento dos bens será de ***60 dias*** a contar da data de adjudicação.

NAZARÉ

MUNICÍPIO DA NAZARÉ
Câmara Municipal

INFORMAÇÃO

O preço base do procedimento, como parâmetro base de preço contratual, é fixado no valor de ***197.600,00€,*** acrescido de IVA à taxa legal em vigor.

Nesse sentido, solicita-se ao Executivo Municipal que:

- Decida autorizar a abertura de procedimento para Aquisição de Bens – Servidor Informático (Datacenter).

Propõe-se ainda, nos termos do n.º 2 do CCP, a delegação de competência no júri para:

- Prestar esclarecimentos;
- Prorrogação do prazo fixado para a apresentação das propostas.

A Técnica Superior,

11-05-2023

Liliana Codinha
Técnica Superior

NAZARÉ

MUNICÍPIO DA NAZARÉ
Câmara Municipal

CONCURSO PÚBLICO

Artigo 20.º, n. º1, alínea b) do Código dos Contratos Públicos (CCP)

CADERNO DE ENCARGOS

Aquisição de Bens – Servidor Informático

(*Datacenter*)

Parte I - Cláusulas Jurídicas

Capítulo I -Disposições gerais

Cláusula 1.ª | Objeto

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar, na sequência do procedimento pré-contratual que tem por objeto principal **Aquisição de Bens – Servidor Informático (Datacenter)**, com as especificações técnicas definidas na Parte II – Cláusulas Técnicas.

Cláusula 2.ª | Preço base

2. O preço base é de ***197.600,00€,*** acrescido de IVA à taxa legal em vigor.
3. O preço base corresponde ao valor máximo a pagar pela execução de todas as prestações que constituem objeto do contrato.

Cláusula 3.ª | Contrato

1. O contrato é composto pelo respetivo clausulado contratual e seus anexos.
2. O contrato integra os seguintes elementos:
   a. os suprimentos dos erros e omissões do Caderno de Encargos, identificados pelos concorrentes, desde que tais 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 presente Caderno de Encargos;
   d. a proposta adjudicada;
   e. os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos nas alíneas a) a e) do 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 e seus anexos, 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.

5. Além dos documentos indicados no n.º 2, o adjudicatário obriga-se também a respeitar, no que lhe seja aplicável, as normas europeias e portuguesas, as especificações e homologações de organismos oficiais e fabricantes ou entidades detentoras de patentes.

Cláusula 4.ª | Duração do contrato

1. O contrato vigorará até à entrega dos bens, em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

2. O prazo de duração do contrato é contado a partir da data da celebração do respetivo contrato escrito, ou da decisão de adjudicação, caso este último tenha sido dispensado.

3. O contrato terá um prazo de execução de ***60 dias***.

Capítulo II - Obrigações contratuais

Secção I | Obrigações do fornecedor

Subsecção I | Disposições gerais

Cláusula 5.ª | Obrigações principais

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrerão para o fornecedor as seguintes obrigações principais:

a. Obrigação de fornecer os bens de acordo com condições fixadas na parte II do presente Caderno de Encargos e de acordo com condições expressas na sua proposta;

b. Obrigação de não alterar as condições do fornecimento de bens;

c. Obrigação de designar um interlocutor responsável pela gestão do contrato, disponível para prestar o devido suporte, bem como quaisquer alterações a essa designação;

d. Obrigação de cumprir com a legislação em vigor e demais legislação que entretanto venha a ser publicada no âmbito do objeto do contrato;

e. Obrigação de não ceder a sua posição contratual sem prévia autorização do Município;

f. Obrigação de prestar de forma correta e fidedigna todas as informações referentes às condições em que é fornecido dos bens, bem como ministrar todos os esclarecimentos que se justifiquem, de acordo com as circunstâncias;

g. Obrigação de dar resposta aos pedidos de informação efetuados pelo Município no prazo máximo de 1 dia útil;

h. Obrigação de, no caso de não ser possível o cumprimento do prazo definido na alínea anterior, o adjudicatário informar o Município, apresentando a devida justificação e proposta de calendarização alternativa;

i. Obrigação de comunicar qualquer fato que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação social, os seus representantes legais com relevância para o contrato, a sua situação jurídica e a sua situação comercial;

j. Obrigação de comunicar antecipadamente ao Município os factos que tornem total ou parcialmente impossível o fornecimento dos bens ou o cumprimento de qualquer outra das suas obrigações.

2. A título acessório, o fornecedor de bens ficará ainda obrigado a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados ao fornecimento dos bens, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Subsecção II | Dever de sigilo

Cláusula 6.ª | Informação e sigilo

1. O cocontratante deve prestar ao contraente público todas as informações que este lhe solicitar e que sejam necessárias à fiscalização do modo de execução do contrato, devendo o contraente público satisfazer os pedidos de informação formulados pelo cocontratante e que respeitem a elementos técnicos na sua posse cujo conhecimento se mostre necessário à execução do contrato.

2. Salvo quando, por força do contrato, caiba ao cocontratante o exercício de poderes públicos, compete exclusivamente ao contraente público a satisfação do direito à informação por parte de particulares sobre o teor do contrato e quaisquer aspetos da respetiva execução.

3. O contraente público e o cocontratante guardam sigilo sobre quaisquer matérias sujeitas a segredo nos termos da lei às quais tenham acesso por força da execução do contrato.

Secção II | Obrigações do Município

Cláusula 7.ª | Preço contratual

1. Pelo fornecimento dos bens objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o Município deverá pagar ao fornecedor dos bens, os bens efetivamente fornecidos, nos termos da Parte II do Caderno de Encargos e de acordo com os preços constantes da lista de preços unitários da proposta adjudicada.

2. O valor total da proposta adjudicada não poderá ser superior ao preço máximo fixado no presente Caderno de Encargos, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.

3. O preço referido no número anterior incluirá todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público (incluindo as despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças).

Cláusula 8.ª | Condições de pagamento

1. As quantias devidas pelo Município, nos termos das cláusulas anteriores, deverão ser pagas após a receção, pelo contraente público, das respetivas faturas, no prazo de 60 dias, as quais só poderão ser emitidas após o vencimento da obrigação respetiva.

2. As faturas emitidas ao Município da Nazaré deverão ser enviadas para o email - faturas@cm-nazare.pt, com a indicação do número do processo de contratação e compromisso.

3. Para os efeitos do disposto no n.º 1, a obrigação considerar-se-á vencida com a entrega dos bens, de acordo com a nota de encomenda.

4. Não poderão ser propostos adiantamentos por conta dos bens a adquirir.

5. Em caso de discordância por parte do Município, quanto aos valores indicados nas faturas, deverá este comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.

6. Desde que devidamente emitidas as faturas e observado o disposto na Cláusula 7.ª e no n.º 1 da presente cláusula, os pagamentos serão efetuados preferencialmente através de transferência bancária.

7. Para o bom e pontual cumprimento das obrigações decorrentes do contrato, e no caso de não ser exigida a prestação da caução, poderá o Município, se o considerar conveniente, proceder à retenção de até 10% do valor dos pagamentos a efetuar, nos termos do artigo 88.º do CCP.

Capítulo III - Penalidades contratuais e resolução

Cláusula 9.ª | Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, o Município da Nazaré pode exigir do co-contratante o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento.

2. Quando as sanções revistam natureza pecuniária, o respetivo valor acumulado não pode exceder 20% do preço contratual, sem prejuízo do poder de resolução do contrato.

3. Nos casos em que seja atingido o limite previsto no número anterior e o Município decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%.

4. Na determinação da gravidade do incumprimento, o Município terá em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do fornecedor de bens e as consequências do incumprimento.

5. As penas pecuniárias previstas na presente cláusula não obstam a que o Município exija uma indemnização pelo dano excedente.

Cláusula 10.ª | Força maior

1. A não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior não será havida como incumprimento, pelo que não deverão, nesses casos, ser impostas penalidades ao fornecedor de bens.

2. Entende-se como casos de força maior o conjunto de circunstâncias que impossibilitem a realização pontual das prestações, 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.

3. Desde que verificados os requisitos do número anterior, poderão constituir casos de força maior, entre outros, acidentes de viação, doença comprovada, os tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

4. Não constituirão casos de força maior:

   a. As circunstâncias que não constituam força maior para os subcontratados do fornecedor, na parte em que intervenham;

b. As determinações governamentais, administrativas ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento, pelo fornecedor de bens, de deveres ou ónus que sobre ele recaiam;

c. As manifestações populares devidas ao incumprimento de normas legais pelo fornecedor;

d. Os incêndios ou inundações com origem nas instalações do fornecedor de bens, cuja causa, propagação ou proporções se devam a culpa ou negligência deste ou ao incumprimento de normas de segurança;

e. As avarias nos sistemas informáticos ou mecânicos do fornecedor, não resultantes de sabotagem;

f. Os eventos que estejam ou devam estar cobertos por seguros.

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

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

Cláusula 11.ª | Resolução por parte do contraente público

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, o Município poderá resolver o contrato, a título sancionatório, no caso de o fornecedor violar, de forma grave ou reiterada, qualquer das obrigações que lhe incumbem, designadamente:

a. Se não forem cumpridas as especificações técnicas e prazos estabelecidas deste Caderno de Encargos;

b. Quando houver recusa expressa no pagamento das penalidades.

2. O direito de resolução referido no número anterior exercer-se-á mediante declaração enviada ao fornecedor e não determinará a repetição das prestações já realizadas, a menos que tal seja determinado pelo Município.

3. A resolução do contrato não invalida o direito a qualquer ação que venha a ser interposta por parte do Município com vista à justa indemnização por perdas e danos eventualmente sofridos com incumprimento do contrato.

Capítulo IV – Seguros

Cláusula 12.ª | Seguros

1. Serão da exclusiva responsabilidade do adjudicatário todas as obrigações relativas ao pessoal utilizado no fornecimento dos bens, assim como, o cumprimento de toda a legislação aplicável, nomeadamente, aquela relativa à celebração de seguros de acidentes de trabalho, ao cumprimento do horário de trabalho e à contratação de trabalhadores imigrantes, bem como a legislação relativa à celebração de seguros de responsabilidade civil.

2. O Município poderá, sempre que entender conveniente, exigir prova documental da celebração dos contratos de seguro referidos no número anterior, devendo o adjudicatário fornecê-la no prazo de 5 dias úteis.

Capítulo V - Resolução de litígios

Cláusula 13.ª | Foro competente

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

Capítulo VI - Disposições finais

Cláusula 14.ª | Subcontratação e cessão da posição contratual

A subcontratação pelo adjudicatário e a cessão da posição contratual por qualquer das partes dependerá da autorização da outra, nos termos do Código dos Contratos Públicos.

Cláusula 15.ª | Responsabilidade

1. O adjudicatário responderá, nos termos da lei, por todos os danos ou prejuízos sofridos pelo Município, seus trabalhadores, operadores ou terceiros, em consequência da adjudicação, devendo para tal celebrar os necessários contratos de seguros, conforme disposto na cláusula 12.ª.

2. Se o Município tiver que assumir a indemnização de prejuízos que, nos termos do presente caderno de encargos, são da responsabilidade do adjudicatário, este indemnizá-lo-á em todas as despesas que, por esse fato e seja a que título for, houver que suportar, assistindo àquele Município o direito de regresso das quantias que tiver pago ou que tiver que pagar.

3. O Município não responderá por quaisquer danos ou prejuízos sofridos pelo adjudicatário, salvo culpa comprovada dos trabalhadores daquele Município, no exercício das respetivas funções.

Cláusula 16.ª | Comunicações e notificações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas deverão ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.

2. Qualquer alteração das informações de contato constantes do contrato deverá ser comunicada à outra parte.

Cláusula 17.ª | Contagem dos prazos

Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados.

Cláusula 18.ª | Legislação aplicável

O contrato é regulado pela legislação em vigor.

Parte II - Cláusulas Técnicas

CLÁUSULA 1.ª

PREMISSAS DE INTEGRAÇÃO

Em virtude do Município da Nazaré já ter em produção alguns sistemas/serviços, asseguram-se as seguintes premissas relativamente à implementação dos equipamentos/*softwares* alvo desta arquitetura tecnológica.

- Os equipamentos apresentados deverão respeitar as normas do Município da Nazaré, e deverão ser integrados na solução existente em produção, diminuindo a curva de aprendizagem dos técnicos.
- A solução de armazenamento deverá suportar as funcionalidades atualmente em produção, tendo em conta as caraterísticas do sistema Storage Area Network (SAN) pretendido. Deverão ser assegurados todos os parâmetros oferecidos pelo sistema SAN, nomeadamente, mas não limitado a balanceamento dinâmico e automático de dados, balanceamento dinâmico e automático de *performance* entre diferentes tipos de *raid* dentro da mesma *pool* de discos, integração da gestão na consola do "*hypervisor*" e configuração da funcionalidade "*thin/thick provisioning*".

Deverão ainda ser garantidas as seguintes premissas de software da matriz de armazenamento:

- Configuração de "*Multi-path*/IO";
- Configuração de software para monitorização de Performance;
- Configuração de software para Integração automática de "*Snaps*" em VSS e VDS;
- Configuração de software "*Hypervisor-aware*" para "*SAN-based snapshots*", clones, replicação e recuperação rápida;
- Configuração de software para "*Undelete" de Volumes/Luns*";
- Configuração de software para Volume/"Lun unmap"-("re-thinning");
- Integração de todo o software e gestão com o domínio existente (Microsoft Windows) das funcionalidades de autenticação da interface de gestão (LDAP/ AD) e da funcionalidade de "*single sign-on*".

Para o efeito, deverá ser apresentada uma declaração do fabricante, atestando a competência técnica do preponente nos equipamentos e gamas propostas, assim como nas gamas já existentes no Município da Nazaré (Dell SC Series e EQL Series).

- Os servidores de suporte à virtualização deverão assegurar a compatibilidade com os servidores existentes, nomeadamente em todas as suas componentes como por exemplo, mas não limitado a

compatibilidade com a camada de software para virtualização, compatibilidade com a componente de rede atualmente instalada e compatibilidade com a plataforma de gestão existente. Para o efeito, deverá ser apresentada uma declaração do fabricante, atestando a competência técnica do preponente nos equipamentos e gamas propostas, assim como nas gamas já existentes (Dell PE R Series).

- A solução de armazenamento deste procedimento deverá ser migrada para a nova infraestrutura. A solução atual deverá passar para ambiente de DR. Para o efeito, deverá ser apresentada uma declaração do fabricante, atestando a competência técnica do preponente nos equipamentos de armazenamento existentes (*Dell Storage Equallogic/ SC Series*).

- A solução de servidores deste procedimento deverá ser migrada para a nova infraestrutura. Os servidores atuais deverão passar para ambiente de DR. Para o efeito, deverá ser apresentada uma declaração do fabricante, atestando a competência técnica do preponente nos equipamentos de computação existentes (*Dell PowerEdge R*).

- A solução de rede ToR atual deverá ser migrada reimplementada em DR. Para o efeito, deverá ser apresentada uma declaração do fabricante, atestando a competência técnica do preponente nos equipamentos de rede existentes (*Dell Networking N e S series*).

CLÁUSULA 2.ª

REQUISITOS GERAIS

São indicados o período de garantia, bem como as condições de manutenção e assistência dos equipamentos e soluções. Considera-se manutenção, o conjunto de operações efetuadas pelo fornecedor tendentes a repor e manter em boas condições de funcionamento da solução proposta, durante a vigência da Garantia/ Suporte.

A reparação de hardware terá lugar sempre no local das instalações da entidade adjudicante, podendo ser retirado o equipamento quando não for viável a sua reparação no local, devendo neste caso ser substituído por outro idêntico, tendo em especial consideração a salvaguarda da informação e bom funcionamento do sistema global.

O fornecedor deve assegurar a continuidade de fabrico e do fornecimento de todas as peças, componentes ou equipamentos que integram os bens fornecidos no âmbito do contrato pelo prazo de 5 anos a contar da assinatura do auto de receção respetivo.

Todos os componentes da solução deverão ser novos e os sistemas com componentes reparados ou recondicionados não são aceites. Deverá ser apresentada declaração da marca, atestando as condições dos equipamentos como novos.

Os equipamentos propostos têm um suporte e garantia mínima de 5 anos, com atendimento 24h por dia/7 dias por semana, com nível de assistência no dia útil seguinte, com técnico no local de instalação.

A componente SAN/ NAS, para alem do especificado, deverá contemplar um *TAM – Technical Account Manager* dedicado e assignado, de língua nativa Portuguesa, diretamente do fabricante, durante os 5 anos de suporte requeridos. A componente SAN deverá contemplar ainda serviço de monitorização proactiva por parte do fabricante, 24h por dia/7 dias por semana, durante 5 anos, do tipo "*call home*", assegurando a monitorização do equipamento 24 horas por dia e 7 dias por semana, garantindo uma resposta pró-ativa no suporte do sistema.

Estão ainda incluídas todas as atualizações e *updates* dos *softwares/firmwares* para as funcionalidades propostas, por um período de 5 anos.

Ainda para a componente SAN, deverá ser apresentada declaração de fabricante atestando que os equipamentos propostos não se encontram em final de vida (EOL).

Em reunião prévia à implementação deverá ainda ser apresentada a calendarização e planeamento de todos os procedimentos necessários da instalação da solução com os tempos de implementação previstos, em concordância com o contratante;

É obrigatória a descrição detalhada das configurações propostas em cada equipamento, incluindo marca, modelo e caraterísticas;

Caso existam, detalhar os requisitos necessários (ex: privilégios de administração, requisitos elétricos, espaço físico, etc.) à instalação.

Deverá ser garantido que a existência de *downtime* na infraestrutura existente, a existir, seja em horário pós-laboral (após 16h00) ou aos fins-de-semana e feriados nacionais/ locais;

Garantir formação *on-job* para colaboradores técnicos do cliente;

Incluir o fornecimento de um documento final detalhando a solução implementada;

Incluir todos os demais equipamentos, software e respetivos serviços de instalação e configuração não contemplados neste documento e necessários à implementação da solução;

A solução proposta deverá ser do tipo "chave na mão".

CLÁUSULA 3.ª

QUANTIDADES E CARACTERISTICAS TÉCNICAS DOS EQUIPAMENTOS

Os equipamentos a propostos no âmbito do presente descritivo técnico apresentam as características mínimas indicadas na tabela IV, que se segue:

Características Mínimas dos Equipamentos

MATRIZ DE ARMAZENAMENTO		
Qtd	**Equipamento**	**Configuração**
1	Sistema SAN/ NAS de produção	A solução a propor deverá conter as seguintes componentes: • **Storage NVMe (SAN e NAS):** disponibilizar uma solução de armazenamento, robusta, segura, escalável e flexível sobre tecnologia NVMeoFC, NVMeTCP, iSCSI; Ethernet (NAS) **Características Hardware Obrigatórias (SAN):** • Uma única consola de gestão para a SAN e NAS (Nativa em HTML 5) • 100% NVMe END-to-END (sem suporte para discos SAS) – inclusive em gavetas externas • Escalabilidade até um mínimo de 8 controladores em cluster/federação geridos nativamente numa única consola, sem impedimentos, com simples adição de "controladores" de processamento variável, sem interrupções e com capacidade nativa de balancear a capacidade de forma inteligente, automatizada e transparente sem interrupção de serviço para os servidores e respetivas aplicações e sistemas operativos. • Sistema escalável até um mínimo de 5.8PB de capacidade RAW • Capacidade de adição de disco unitário para futuros upgrades de capacidade com unidades de disco de capacidade diferente (superior) da originalmente adquirida. • Expansão de disco até 380 discos NVMe (NAND) • Pretende-se um equipamento com fiabilidade nativa em 2 controladores de 99.9999% (6x noves) com capacidade de expandir até 99.99999% (7x noves) com mecanismos metro cluster nativo • Suporte obrigatório no mínimo aos seguintes níveis de RAID 5 ou RAID6 e com sistema de hotspare distribuídos com um rácio mínimo de 25:1 com capacidade de adicionar granular um disco de cada vez em caso de upgrade, mesmo de tamanho diferente dos existentes • Suporte a Hotspare integrado (distribuído) com capacidade de regeneração automática e instantânea (na existência de pelo menos 20%

		de espaço disponível) em caso de falha de discos e até estes serem substituídos, aumentando a resiliência e proteção dos dados por perda de discos. • 2x Módulos de processamento (controladores redundantes) activo-activo com um mínimo 2x Processadores Físicos. Um total mínimo de 24x cores de processamento por par de controladora. Pretende-se capacidade combinada integrada de cache (DRAM) mínimo de 192GB. A cache deverá ser nativa dos controladores sem expansões através de discos Flash/NAND, NVRAM, SCM – NVMe • É requerido que o sistema tenha por par de controladores mecanismo dedicado para fazer offload da deduplicação e compressão não usando as cores (24x) assignados para os controladores. o Possibilidade de verificação ao nível da LUN do nível de redução de dados com a análise informativa de dados únicos • Segurança do Firmware com TPM (trusted Plataforme Module) assinatura X.509 ou superior. • Suporte Suporte Secure Boot/UEFI (Intel Boot guard) • Segurança ativa de dados (DARE) - Pretende-se uma solução com discos (total proposto e upgrades futuros) do tipo SED (encriptados nativamente) FIPS 140-2 o Suporte para chave de encriptação interna ou Externa (KMIP) • Os discos deverão ser NVMe com dual port para garantir as leituras e escritas pelos controladores em simultâneo • FrontEnd - Um total mínimo de 8x portas SFP28 (25Gb/s), com suporte para NVMeTCP e 8x portas FC (32Gb/s) NVMeoFC. • FrontEnd expansão – Capacidade de expansão para portas adicionais (FC16, FC32 NVMeoFC, NVMeTCP, iSCSI 10Gb/s, 25Gb/s, 100Gb/s) dentro de apenas um par de controladores. • Suporte NVMeTCP a Centralized Discovery Controller (CDC) • Discos, fontes de alimentação, ventiladores, processadores e portas de comunicação (FC NVMEoFC /iSCSI NVMeTCP, Ethernet) redundantes do tipo hot-swap; • Permitir combinar discos NVMe SSD e Storage Classe Memory para dados, encriptados e de porta dupla (acesso activo-activo em simultâneo aos discos) no cluster e movimentar dados entre eles, sem disrupção de serviço; • Suporte de garantia de 5 anos (24x7xNBD) e independente por módulo e por gaveta de discos adicionada no futuro. • Possibilidade de Integração e retro-compatibililidade com modelos de cluster anteriores e futuros, independente de características ou funcionalidades na integração na SAN.

		• Fornecimento Software de monitorização cloud com suporte e manutenção total por parte do fabricante do hardware proposto devendo podendo incluir a rede de comunicações da SAN e servidores, monitorização dos Servidores, sistemas de backup. • Discos requeridos para a Solução de Produção: • 10 discos de 1.92TB SED (encriptados) NVMe SSD 2,5" Dual Port • Deverão ficar disponíveis no mínimo 15 slots de disco para expansão futura. Se necessário deverá ser proposta gaveta de discos adicional. ➢ **Software SAN Obrigatório.** • Deverá permitir tecnologia Redirect on Write para SnapShots e clones por/volume ou grupo de volumes semanais com períodos de retenção de 15 dias e réplicas diárias • Possibilidade de visualizar a topologia do volume com os snapshots associados • Deverá ser fornecido software para movimento automatizado de volumes entre todos tipos de discos diferentes (Volume tiering), em cluster • Tenologia para disaster recovery nativo • Pretende-se nativamente deduplicação e compressão inline sempre ligada globalmente (para todos os dados do array e não apenas por volume) para todas as operações da SAN e NAS (volumes) sem impacto de latência ou perda de desempenho com uma granularidade de blocos de 4K • Deverá ser fornecido software para recuperar espaço previamente ocupado e permitir a sua reintegração dinâmica no espaço disponível. • A configuração do RAID deve ser feita de modo dinâmico e automático pelo sistema em função dos requisitos do solicitados pelo Host ou aplicações. • O sistema de gestão de Hotspare distribuído deve ter a capacidade de recriar automaticamente um novo hotspare distribuído em caso do inicial ter sido usado, aproveitando espaço disponível, aumentando a segurança dos dados até o disco em falha ser substituído. • Deverá ter a capacidade de balancear automaticamente os dados pelos discos de forma a consumir menos células, consequentemente diminuir o "gasto" dos discos NAND. • Suporte integrado para VVols com suporte a NVMeFC (NVMe-vVol)

		• Deverá ser fornecido software para Thin/Thick provisioning. • Deverá ser fornecido software para QoS (Quality of Service). • Deverá ser fornecido software para compressão e deduplicação (SAN/NAS) • Deverá ser fornecido software para monitorização de Performance, volumes, portas, discos, replicações e Hardware com histórico (mínimo 24 meses) sem recorrer a servidores ou serviços externos. • Capacidade de replicação vVols (VASA 3.0) com suporte a point in time replica (PiT) com integração SRM • Capacidade nativa de replicação Metro ativo-ativo bidirecional o Suporte para balanceamento ativo VMware Streched cluster o Suporte para cross-site FT (Fault Tolerance / hotstand-by) o Suporte VMware HA o vMotion / Storage vMotion across site border o Suporte a hosts ligados a um único array ou ambos os arrays (non-uniforme / Uniforme host conectivity) • Capacidade de escolha para Instalação (durante a inicialização) de linguagem português ou Inglês para a consola de gestão nativa (HTML5) do array fornecido ➢ **Software SAN/Servidor para Integração aplicacional dos servidores, obrigatório.** • Deverá ter integração para Hyper-V • Deverá ter integração para VMware ESX (VAAI) • Deverá ser fornecido software para integração automática de Snapshots e Clones com consistentes com MS VSS/VDS para SQL, Exchange, Sharepoint (MOSS), File Service. • Deverá ser fornecido software para integração automática de Snapshots e Clones com consistentes com VMware ESX • Deverá suportar o rebalanceamento de dados entre arrays dentro do mesmo Cluster/federação sem disrupção de serviço par o host / sistemas operativos e aplicações • Deverá ser fornecida um mínimo de ferramentas para PowerShell / Kubernetes / VRops / Ansible. • Software de migração de dados de outros equipamentos deverá ser nativo ou incluído na proposta, não trazendo custos adicionais para o projeto

		➢ **Software NAS** • Deduplicação e compressão inline global ao array • Deverá ser fornecido software para Snapshots e Clones • Suporte para: Common Event Enabler (CEE) • Common Agente Anti-Virius (CAVA) • Common Event Publishing Agente (CEPA) / SMB e NFS • Deverá suportar mínimo os seguintes protocolos: NFS 4.1; SMB 3.11; SFTP • Tecnologia WORM (Write Once Read Many) com suporte granular ao nível do Folder da norma SEC 17a-4(f) • Capacidade de replicação nativa de file assíncrona bidirecional integrada na replicação do array (bloco e File) o Capacidade de Reverter sessão de replicação o Fazer clone da replica o Modificação da replica destino o Adição de novos File systems à replica o Fazer pausa e retomar a replica o Planear sessões de failover o Suporte IPV4 / IPV6 • Suporte para Host VMware NFS file Systems datastores (io size 8k, 16k, 32k, 64k) o Suporte a asyncMtime por defeito o Snapshot Suporte o VMDK Fast clone ***Nota importante*:** O licenciamento do software fornecido do array, deverá contemplar um número de servidores e aplicações ilimitado. Deverá ser fornecido um sistema de monitorização com histórico até 2 anos e capacidade para monitorizar o array NVMe fornecido e que suporte no futuro para componentes SAN switches, servidores, backup appliances na mesma consola durante a vigência da garantia solicitado nos equipamentos a adquirir. ***Notas adicionais obrigatórias*:** Deverá estar incluído na Garantia do Storage Hardware/Software/host suporte pro-activo, call home, update de versões do firmware e software.

		Requisitos de garantias, manutenção e suporte A solução a fornecer deverá contemplar: • Hardware (todas as componentes de hardware): o Manutenção e suporte pelo período mínimo de 5 anos, a contar da data de instalação; o Suporte 24h x 7 dias x NBD tempo de resposta no site principal e dia útil seguinte no site de recuperação; o A Manutenção será obrigatoriamente prestada pelo fabricante durante os 5 anos de vigência do contrato. • Software (todas as componentes de software): o Upgrade de versões, Manutenção e suporte pelo período mínimo de 5 anos, a contar da data de instalação; ***Serviços:*** Deverão ser contemplados obrigatoriamente os seguintes serviços: • Instalação física, configuração e integração na infraestrutura existente de todo o hardware fornecido; • Gestão e Acompanhamento de Projeto; • Garantir um interveniente dedicado na qualidade de gestor de projeto, interpelando necessidades e garantindo o acompanhamento em tempo real do mesmo; • Deve ser garantido a passagem de conhecimento para operação dos equipamentos e software propostos a pelo menos um técnico nomeado pelo adjudicante. • Todos os demais serviços não contemplados neste documento e necessários à implementação da solução devem ser apresentados e notificados de forma clara.

Qtd	Equipamento	Configuração
		CLUSTER DE VIRTUALIZAÇÃO
2	Servidores de Produção (nó de virtualização)	a) Servidor denso de 1U de instalação em rack 19''; b) 2 Processadores tipo Intel ou equivalente, cada um com 8 cores/ 16T, de 3.6GHz TMax de velocidade de relógio máxima e 12MB de cache independente por processador, com suporte para memória a 2933MTs; c) 512GB de RAM a 3200MTs RDIMM expansível até 1024GB de RAM. Ficarão disponíveis no mínimo 8 slots para expansão futura; d) 2 chips de armazenamento do tipo "boss card" M.2 com controlador, de 480GB em RAID1 (SO/ virtualizador); e) 2 interfaces de rede 25GbE com interfaces SFP28; f) 2 interfaces HBA FC 32Gb com módulos óticos instalados; g) Suporte para opção Placa de rede, opção entre 4 x 1GE ou 2 x 10GE + 2 x 1GE ou 4 x 10GE ou 2 x 25GE na motherboard; h) 1 Placa de gestão de sistema avançada de gama enterprise com as seguintes funcionalidades mínimas: o Consola e Media Virtuais com colaboração, permitindo acesso para shut down, start up e acesso a parâmetros de pré-arranque e BIOS, mesmo com o equipamento desligado. o Monitorização e estimativa de consumos elétricos. o Placa NIC dedicada. o Capacidade de diagnóstico com captura do ecrã de crash. o Autenticação dois fatores. o Configuração e atualização local e remota. o Suporte de Serviços de Diretoria. o Capacidade de Scripting. o Capacidade de recomendação de substituição de peças. o Instalação remota de sistema operativo. o Syslog Remoto Gestão básica de hardware via IPMI 2.0. o Playback de vídeo de Crash. o Captura de Boot o Diagnósticos embutidos o Monitorização da alimentação da plataforma o Ferramenta embutidas de instalação de sis. Operativo. o Acesso por Web GUI e linha de comando; i) Fonte de alimentação redundante, Hot Plug, com potência dimensionada para as necessidades e respetivos cabos de alimentação; j) Sliding Rails com mecanismo de gestão inteligente de cabos; k) Suporte de 5 anos, 24/7, com intervenção de técnico no local, no máximo no próximo dia útil. l) Suporte para opção Switch idependent partinioning

		m) Suporte para opção de drives encriptadas de origem n) TPM 2.0 o) Software de gestão e controlo p) São suportados no mínimo os seguintes sistemas operativos: Canonical® Ubuntu® LTS, Citrix® XenServer®, Microsoft Windows Server® with Hyper-V, Red Hat® Enterprise Linux, SUSE® Linux Enterprise Server, VMware® ESXi. q) Integração aplicacional com: Microsoft® System Center, VMware® vCenter™, BMC Software. r) Compatibilidade de conexão com: Nagios & Nagios XI, Oracle Enterprise Manager, HP Operations Manager, IBM Tivoli Netcool/OMNIbus, IBM Tivoli® Network Manager, CA Network and Systems Management

Qtd	Equipamento	Configuração
		SWITCH ToR
2	ToR Switch	a) Montagem em rack de 19" (1U); b) Cada Switch disponibiliza 12 portas utilizáveis em FULL fabric (line rate nas portas não partilhadas) 10Gb/s autosence (1/10) em formato SFP+ e ainda 3 portas 100Gb/s em formato QSFP28; c) Permite expansão futura em cada chassis até no mínimo 24 portas SFP+ 10Gb/1Gb ou 12 portas SFP28 25Gb ou 3 portas QSFP+ 40Gb ou 6 portas QSFP28 50Gb. Todas as normas deverão ser suportadas em alternativa de crescimento; d) Cada Switch inclui fontes de alimentação redundantes; e) O Switch fabric capacity de cada switch é 800 Gbps e o Forwarding rate é 600Mpps; f) Suporta Link Aggregation, no minimo 128 Grupos LAG; g) Suporta no mínimo 4000 VLANs; h) Suporta Layer 2 switching; i) Suporta Layer 3 routing (static routes, RIP, OSPFv2, OSPFv3, BGP, PBR); j) Suporta Multicast; k) Suporta todos os standards no que concerne a gestão de qualidade de serviço, gestão de redes e gestão da segurança; l) Inclui suporte para os standards: i. IEEE 802.3ab – 1000 Base-T ii. IEEE 802.3ac – VLAN tagging iii. IEEE 802.3ad – Link aggregation iv. IEEE 802.3ae – 10 Gigabit Ethernet (10GBASE-X)

		v. IEEE 802.1D – Spanning Tree vi. IEEE 802.1S – Multiple Spanning Tree vii. IEEE 802.1W – Rapid Spanning Tree viii. IEEE 802.1Q – Virtual LANs with Port-based VLANs ix. IEEE 802.1v – Protocol-based VLANs x. Suporte Open Network Install Environment (ONIE) xi. Suporte para VXLAN layer 2/layer 3 gateway Deverá permitir Open Networking & SDN, com suporte para pelo menos os seguintes SOS: ➢ **Open Source:** o The Linux Foundation o Openswitch o SONiC o SAI ➢ **Open Ecosystem:** o Cumulos Networks o Big Switch Networks o IPinfusion o Midokura o Nuagenetworks o Open Daylight o ONOS o Pluribus Networks o VMWARE NSX m)Suporta MTU de 9K (jumbo frames); n) Contempla ventilação redundante e de velocidade variável; o) Suporte de 5 anos, 24/7, com intervenção de técnico no local, no máximo no próximo dia útil. A garantia abrange as fontes de alimentação, ventoinhas de refrigeração e módulos óticos e cabos SFP, SFP+ e QSFP+, SFP28 e QSFP28. Ao abrigo do suporte está contemplado o acesso a updates de firmware.

Qtd	Equipamento	Configuração
		SWITCH SAN
2	SAN Switch	a) Montagem em rack de 19" (1U); b) Cada Switch disponibiliza 24 portas 32Gb/s Fibre Channel Small Form Factor Pluggable; c) Cada switch deverá incluir no mínimo 8 módulos óticos 32Gb/s Fibre Channel Small Form Factor Pluggable; d) Frame Buffer 2k dinamico; e) Classe de serviço Class 2, Class 3, Class F f) Tipo de portas: F_Port, E_Port, M_Port, D_Port (ClearLink Diagnostics Port) on 24 SFP+ ports; Access Gateway mode: F_Port and NPIV-enabled N_Port; g) Serviços Fabric: BB Credit Recovery; Brocade Advanced Zoning (Default Zoning, Port/WWN Zoning, Peer Zoning); h) Congestion Signaling; Dynamic Path Selection (DPS); Extended Fabrics; Fabric Performance Impact; i) Notification (FPIN); Fabric Vision; FDMI; Flow Vision; F_Port Trunking; FSPF; j) Integrated Routing; ISL Trunking; Management Server; Name Server; NPIV; NTP v3; Port; k) Decommission/Fencing; QoS; Registered State Change Notification (RSCN); Target-Driven Zoning; Traffic; l) Optimizer; Virtual Fabrics; VMID and AppServer. m) *Gestão:* Advanced Web Tools. SSH, Auditing, Syslog NTP v3, CLI, SMI-S compliant; REST API, HTTP, SNMP v1/v3 (FE MIB, FC Management MIB) n) *Acesso para gestão*: 10/100/1000 Mb/s Ethernet (RJ-45), In-band over Fibre Channel, Serial port (RJ-45), USB port; o) *Segurança:* DH-CHAP (between switches and end devices), FCAP switch authentication; HTTPS, IPsec, IP filtering, LDAP with IPv6, Open LDAR, Port Binding, RADIUS, TACACS+, user-defined Role-based Access Control (RBAC), p) Secure Copy (SCP), Secure RPC, Secure Syslog, SSH v2, SSL, Switch Binding, Trusted Switch q) *Diagnóstico:* ClearLink optics and cable diagnostics, including electrical/optical loopback, link traffic/latency/distance, flow mirroring; built-in flow generator, POST and embedded online/offline diagnostics, including environmental monitoring, FC ping and Pathinfo (FC traceroute), frame viewer, non-disruptive daemon restart, optics health monitoring, power monitoring, RAS trace logging, and Rolling Reboot Detection (RRD); r) Integração "Call Home"

		s) Equipamento deverá ser da mesma marca do equipamento NAS/ SAN e dos Servidores; t) Suporte de 5 anos, 24/7, com intervenção de técnico no local, no máximo no próximo dia útil. A garantia abrange as fontes de alimentação, ventoinhas de refrigeração e módulos óticos e cabos SFP, SFP+ e QSFP+, SFP28 e QSFP28. Ao abrigo do suporte está contemplado o acesso a updates de firmware.

ACESSÓRIOS/ PASSIVOS

No âmbito do presente descritivo técnico, são propostos os seguintes acessórios/ passivos:

Acessórios

Qtd	Equipamento	Configuração
ACESSÓRIOS		
16	Cabos Interligação	Cabo SFP+ to SFP+, 10GbE, Copper Twinax Direct Attach Cable, para interligação entre os servidores virtualizadores, SAN/ NAS e switch ToR, sendo portanto da mesma marca dos referidos equipamentos de virtualização, herdando as suas caraterísticas de suporte/ garantia, quer da componente de switch, quer da componente de servidor/ SAN/ NAS.
8	Cabos Interligação	3M OM4 Fiber Cable LC-LC
2	Cabos Interligação	Cabo QSFP28 to QSFP28, 10GbE, Copper Twinax Direct Attach Cable, para interligação entre os switch ToR, sendo portanto da mesma marca dos referidos equipamentos de virtualização, herdando as suas caraterísticas de suporte/ garantia, quer da componente de switch.

SOFTWARE

No âmbito do presente descritivo técnico, são necessários os seguintes softwares:

Qtd	Equipamento	Configuração
SOFTWARE		
1	Plataforma de monitorização e predição de necessidades	➢ Solução de monitorização e previsão de necessidades de toda a infraestrutura. ➢ Deverá permitir notificações proativas, preditivas e análises que identifiquem desvios e impactos de desempenho na solução e sugestão de resolução de problemas.

		➢ Deverá permitir planeamento antecipado relativamente a parâmetros de consumo e tempo provável para esgotamento de recursos, socorrendo-se de tecnologia de AI/ ML para o efeito. ➢ Deverá permitir visão Holística de todo o ambiente, identificando problemas de performance, problemas de avaria, desatualização de drivers, firmwares ou softwares. ➢ Deverá permitir a categorização e a priorização de resolução com base em AI/ ML, identificando as situações mais críticas ou eminentes. Análise de impacto de desempenho e deteção de anomalias: Deverá usar AI e ML para analisar anomalias de performance e permitir remediação imediata. ➢ Análise de contenção de carga de trabalho: Deverá identificar as cargas de trabalho que estão em competição por recursos partilhados e necessitem de ser redistribuídas "noisy neighbor", ajudando a otimizar as cargas mais importantes. ➢ Integração VMware: Deverá fornecer análise de ambientes virtualizados, ajudando a entender as relações VM-armazenamento e o impacto em toda a transação de dados. ➢ Previsão de capacidade total: Deverá permitir efetuar previsões com a antecedência mínima de 3 meses de esgotamento de recurso de armazenamento. ➢ Previsão de capacidade: Deverá prever o consumo de recursos de armazenamento com base em períodos temporais pré-selecionados, facilitando o planeamento de investimento futuro do crescimento da capacidade de armazenamento de dados. ➢ Deteção de anomalias de capacidade: Deverá identificar um aumento repentino de utilização da capacidade que poderia resultar em iminente indisponibilidade de dados. ➢ Notificações: Deverá enviar proactivamente notificações e recomendações por meio de e-mail e ser acessível em qualquer lugar / a qualquer hora via aplicação

		para dispositivo móvel. Deverá permitir personalização, agendamento e partilha de relatórios com a equipa de IT; ➢ Deverá permitir análise de cyber segurança relativamente a versões de software e firmware que tenham vulnerabilidades conhecidas e sugerir remediação. ➢ Deverá permitir gerir o ciclo de vida dos equipamentos, controlando parâmetros de fim de serviço, renovação de serviço e fim de vida de equipamentos. ➢ Deverá permitir reclamar espaço de armazenamento disponível. ➢ Deverá ser compatível com os equipamentos e soluções apresentadas, nomeadamente: ▪ Novo Sistema SAN ▪ Serviços a correr nos nós de virtualização ▪ Novos Nós de virtualização ▪ Plataforma de VMWARE ▪ SAN Switches e ToR Switches ▪ Repositórios de backup ***Suporte e Manutenção:*** O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado diretamente e por um único fabricante com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção pretendida é a seguinte: • Manutenção de 5 anos 24x7 incluindo atualizações e suporte • Prestação de assistência contínua até à solução da avaria. O suporte deverá ser dado diretamente pelo fabricante localmente (preferencialmente em língua portuguesa) sem recorrer a qualquer parceiro para esse efeito.
1	Software de virtualização Produção	VmWare vSphere Essentials Plus Kit, 6CPU (max 32 cores/CPU socket) ou equivalente, com 5 anos de suporte 24/7
1	Software de virtualização Disaster recovery	VMware vSphere 8 Essentials Kit for 3 hosts (Max 2 CPU per host, 32 cores/CPU) ou equivalente, com 5 anos de suporte 24/7
1	Software Microsoft	2 x Windows Server 2022 Datacenter,16CORE ou equivalente 2 x Media Kit WS2016 DC Downgrade w/DVD Media,Multi Lang ou equivalente 2 x Media Kit WS2019 DC Downgrade w/DVD Media,Multi Lang ou equivalente

		80 x Windows Server 2022/2019 User CALs (Standard or Datacenter) ou equivalente
1	Software de replicação com automação de DR	Software deverá proteger Máquinas virtuais (VM) em granularidade de nível de VM com local e replicação remota para recuperação em qualquer Point-in-Time (PiT). Deverá suportar replicação síncrona e assíncrona em qualquer distância com a utilização eficiente da largura de banda WAN. Deverá simplificar a recuperação de desastre, testes de recuperação (DR) e recuperação operacional com recursos de orquestração e automação diretamente acessíveis a partir do VMware vCenter. Deverá fornecer fluxo de de DR automatizado aumentando a eficiência operacional de proteção e recuperação. Deverá adicionalmente permitir a replicação para AWS e VMware Cloud na AWS. ✓ ***Especificações de integração com VMware vCenter*** Deverá ser uma solução totalmente virtualizada, apenas de software, implementada em ambientes VMware vSphere sem qualquer dependência de hardware adicional. Mais ainda, deverá ser uma solução completamente agnóstica ao tipo e marca do hardware que se encontra a montante ou a jusante da replicação. Deverá incluir plug-in para gestão direta em VMWARE vCenter. Deverá ainda permitir automação e orquestração pela mesma via. Deverá replicar a componente de bloco do site produção para o site de DR. ✓ ***Licenciamento de Software:*** 60 VMs ***Suporte e Manutenção:*** O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado diretamente e por um único fabricante com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção pretendida é a seguinte: • Manutenção de 5 anos 24x7 incluindo atualizações e suporte • Prestação de assistência contínua até à solução da avaria. • O suporte deverá ser dado diretamente pelo fabricante localmente (preferencialmente em língua portuguesa) sem recorrer a qualquer parceiro para esse efeito.

SOLUÇÃO DE BACKUP		
1	Solução de backup de dados e tecnologia de repositório de dados	• **Solução de Proteção de Dados:** o A solução de proteção de dados a propor deverá permitir 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. • **Licenciamento da solução de proteção de dados:** o O licenciamento da solução de proteção de dados a propor deverá permitir 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. o Pretende-se a aquisição de um licenciamento totalmente flexível por forma a permitir um melhor enquadramento na realidade da infraestrutura, nomeadamente ao suporte da infraestrutura de virtualização: ▪ Licenciamento por CPU socket físico, independentemente do número de máquinas virtuais alojadas na infraestrutura de virtualização ou do volume de dados a proteger; ▪ Licenciamento por CPU socket físico, capaz de cobrir as necessidades do parque de máquinas físicas, elegíveis para proteção de dados; ▪ 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. ▪ O licenciamento proposto deverá ser perpétuo e propriedade do Município da Nazaré • **Características e requisitos técnicos da solução de backup:** o 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 origem; ▪ Backups completos com recurso a tecnologia de proteção com base somente nas alterações entre cada backup, permitindo a recuperação completa e/ou granular a partir de qualquer ponto no tempo; ▪ 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 (incluindo a possibilidade de garantir Continuous Data Protection) com granularidade ao nível de máquinas virtuais, selecionando 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, através de mecanismos de Secure Multi-tenancy e encriptação; ▪ Integração nativa, por intermédio do VMware vSphere Web Client, da componente de proteção de dados, incluindo as capacidades de gerir operações de backup, recuperação, reporting e replicação de 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 cooling (N+1), fontes de alimentação hot-swappable, memória protegida por bateria (para acautelar 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 suportada a partir de um único fabricante;

		• **Licenciamento de Software:** o 5 CPU Sockets (virtualizadores + NAS) • Capacidade de performance e escalabilidade necessárias para assegurar proteção de investimento e futuras necessidades: o 2 Appliances físicas (uma para produção e outra para Disaster Recovery) com, no mínimo, 32 TB úteis cada uma (excluindo mecanismos de eficiência) o Capacidade de escrita correspondente a pelo menos 7TB/hora o Suporte para protocolos NFS/CIFS, VTL e OpenStorage (e em simultâneo se necessário); o Capacidade de backup direto para o repositório de dados, sem recurso a software de backup, para aplicações Oracle, SAP, SAP HANA e Microsoft SQL; o • 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; • 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); • Deverá incluir todos os componentes e licenciamento necessários para instalação numa cloud pública (AWS, Azure, Google Cloud) • A solução deverá ser fornecida sem limites de clientes e/ou agentes aplicacionais; • A solução deverá oferecer redundância através de tecnologia de replicação para efeitos de Disaster Recovery, que permita garantir a recuperação dos dados em caso de falha/desastre da solução de produção, de forma transparente; • A replicação deverá ser encriptada e efetuada no menor espaço de tempo possível, por forma a permitir o backup regular dos archive logs e salvaguarda dos mesmos por via de replicação;

		• Deverá incluir todos os componentes e licenciamento necessários para permitir a encriptação in-line dos dados escritos • 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: o Fontes de alimentação redundantes o Proteção de disco de dupla paridade (RAID6) o Mecanismo de verificação de integridade dos dados durante a escrita • A solução deverá ainda ser fornecida com pelo menos 2 repositórios respeitando os seguintes requisitos: o Serem capazes de armazenar especificamente dados de backup no formato do software de backup; o Implementação de elevadas taxas de deduplicação (normalmente 10:1 ou mais); o 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; o 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 Gatrner Group.** ➢ ***Integrações e suportabilidades*** Deverá ser proposta uma nova solução de proteção de dados, capaz de permitir ao Município da Nazaré integrar de forma nativa com as principais aplicações e ambientes de virtualização, criando valor através de agilidade e flexibilidade, ao mesmo tempo que permitirá reduzir o esforço de gestão diário da nova solução. 1) Capacidade de integração nativa com ambientes virtualizados VMware por forma a: a. permitir a gestão e operação diretamente a partir do UI de gestão nativo vSphere Web Client; b. Integração com blueprints de VMware, por forma a permitir aprovisionamento de proteção de dados diretamente a partir do catálogo de serviços; c. Suporte multi-tenant

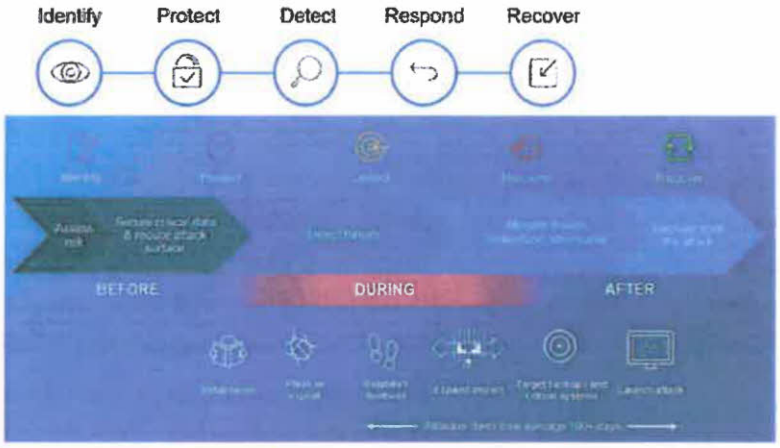
		2) Suporte para API REST para integração com portais de gestão e aprovisionamento; *Suporte e Manutenção:* O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado diretamente e por um único fabricante com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção pretendida é a seguinte: • Manutenção de 5 anos 24x7 incluindo atualizações e suporte • Prestação de assistência contínua até à solução da avaria. • O suporte deverá ser dado diretamente pelo fabricante localmente (preferencialmente em língua portuguesa) sem recorrer a qualquer parceiro para esse efeito.

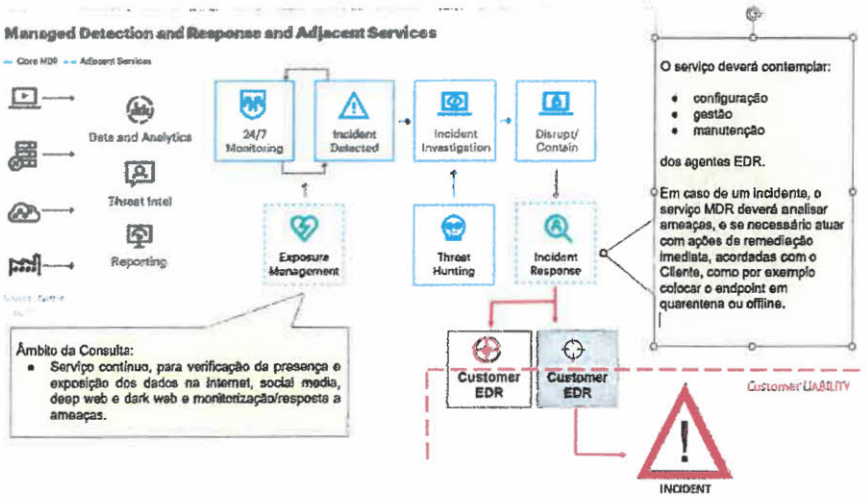
SEGURANÇA

No âmbito do presente descritivo técnico, estão incluídos os seguintes serviços:

Qtd	Equipamento	Configuração
SERVIÇOS SEGURANÇA		
1	Serviços de Operação e Gestão de Eventos de Cibersegurança "Managed Detection and Response Security Operation Center" (SOC as a Service) 24/7	• Especificação do Serviço • O crescente desafio que os ciber ataques a endpoints, servidores, aplicações, redes e workloads de cloud, têm gerado imensos volumes de alertas e falsos positivos que, rapidamente sobrecarregam as equipas de segurança e de operação de infraestruturas de TI. • Da mesma forma, os agentes de ameaças e atacantes maliciosos continuam a desenvolver as suas técnicas, contornando agilmente os mecanismos de prevenção e proteção existentes. Proteger adequadamente os ambientes de TI, requer monitorização constante 24x7, 365 dias por ano e uma resposta imediata por especialistas dedicados e qualificados. • Os agentes de ameaças modernos são metódicos, investindo semanas ou meses a estudar como obterão acesso a aplicações e dados valiosos. Detecção e resposta são elementos essenciais de um programa abrangente de segurança cibernética, conjuntamente com formação contínua de colaboradores, avaliações de segurança cibernética, testes de vulnerabilidade e intrusão, resiliência e planificação de uma eventual recuperação.

		• Proteger as atuais infraestrutras contra as ameaças, exige um investimento em talentos, ferramentas e operações que, muitas vezes, é difícil manter com recursos internos de uma organização. Por este facto, muitas empresas no mercado estão cada vez mais a considerar soluções geridas de detecção e resposta a ataques (X/MDR – Managed Detection & Response), fornecidas por prestadores de serviços externos especializados, que não só garantem uma proteção eficaz como uma contínua atualização técnica do serviço e agentes que o operam. • A prestação de serviços de MDR exige a criação de operações de segurança e o estabelecimento e refinamento de processos. Além disso, os analistas precisam de ferramentas de partilha de conhecimento e formação regular, para se manterem atualizados sobre as ameaças e técnicas mais recentes. • O lado humano da equação MDR exige um grupo de profissionais, com anos de experiência em segurança cibernética, e habilidades como administração de sistemas, análise forense cibernética, investigações de ameaças e testes de intrusão. • Embora muitos prestadores de serviços anunciem e disponibilizem serviços geridos de detecção e resposta a incidentes, apenas alguns têm a capacidade real, credibilidade e recursos técnicos, necessários para oferecer um serviço de excelência. • Estando cientes dos riscos atuais e definindo este tópico como uma das nossas prioridades, o Município da Nazaré iniciou um processo de organização, de recolha e análise de eventos de modo a monitorizar, detetar e conseguir reagir a incidentes de segurança. O objetivo principal é conseguir ter um serviço proactivo, que recolha todos os eventos gerados por equipamentos (fontes) considerados críticos, e que os mesmos sejam enviados para uma plataforma única inteligente, que analise, correlacione e reporte em caso de incidente. • Pretende-se assim, um serviço que siga as metodologias e atue ao nível da deteção e resposta da framework de ciber segurança da NIST, que se adeque às recomendações e normativas do Decreto Lei nº65/2021 do Estado Português, que siga as boas práticas da recente diretiva Directiva de Segurança das Redes e da Informação (NIS2) da União Europeia, e que auxilie na eficaz interlocução com o Centro Nacional de Cibersegurança (CNCS).

		NIST Cyber Security Framework  • A figura seguinte, resume os objetivos pretendidos pelo Município da Nazaré, com a aquisição do serviço MDR. O proponente deverá acautelar estas características e ter a capacidade de entregar um serviço, baseado numa plataforma XDR inovadora (eXtended Detection & Response), com uma equipa de especialistas, devidamente certificados: • Gestão de risco, para melhorar posturas defensivas. • Gestão e suporte, que reduza a complexidade e análise das soluções de segurança. Visibilidade, em todas as tecnologias/infraestruturas de uma organização. • Detecção e bloqueio, até mesmo das ameaças mais avançadas. • Capacidade de resposta, para minimizar o tempo de atuação dos atacantes e respetivos danos. • Percepções, para informar as decisões e ações mais críticas de segurança e um Portal de reporting, para visualizar a correlação de logs, tendências e tomadas de decisão. • Automação contínua, nas ações de prevenção/defensivas e resposta a incidentes.

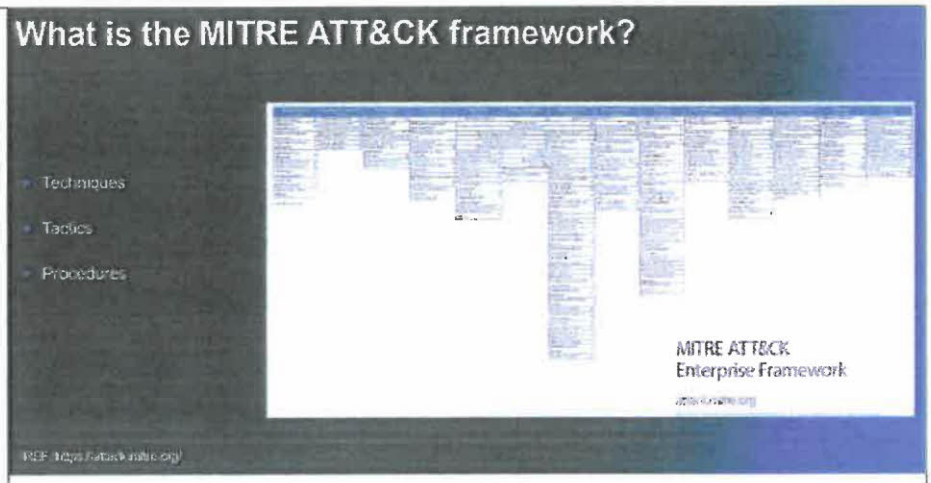


➢ Infraestrutura Atual

- Neste subcapítulo, o Município da Nazaré lista a realidade atual da sus infraestrutura, nomeadamente:
- 80 colaboradores ligados à sua infraestrutura (internos / externos)
- 120 endpoints a proteger (desktops, notebooks, instâncias VDI, servidores físicos ou virtuais)
- deverá integrar com o anti-virus em produção, VMWARE Carbon Black NGAV Standard
- deverá integrar com o EDR em produção, VMWARE Carbon Black EDR Standard
- deverá integrar com a atual firewall em produção, SonicWall
- deverá integrar com os atuais switches de rede em produção, Dell Networking

		➢ *Âmbito do Serviço:* • O Município da Nazaré pretende adquirir um serviço MDR que inclua a recolha, análise, monitorização, correlação e alerta/mitigação dos eventos gerados, em regime 24x7, por parte de uma equipa qualificada, com envio regular de relatórios de cibersegurança. • Este serviço deverá incluir, pelo menos, as seguintes catacterísticas: • Coleta de eventos de segurança • Envio e armazenamento (pode ser temporário – pelo menos 12 meses) dos eventos • Análise, correlação, reação e monitorização dos eventos • Geração de alarmes e alertas • Geração periódica de reports ou dashboards • Sugestão de pontos de melhoria e aconselhamento de segurança • Reuniões de ponto de situação periódicos (mínimo 1 reunião trimestral) • Como requisitos do serviço, o proponente deverá respeitar os pontos seguintes. • Recursos Humanos • Uma equipa global de analistas de segurança (agentes MDR), altamente especializados e certificados na plataforma XDR proposta, com experiência em todas as fases de detecção e mitigação de ameaças, incluindo descoberta de ameaças e vulnerabilidades, segurança de endpoints e resposta e recuperação de incidentes. • O proponente deverá especificar as localizações dos SOCs e das diversas equipas de agentes de nível 1 e nível 2 (análise e investigação de alertas), bem como listar as certificações quer ao nível da ciber segurança, quer ao nível de produtos de diversos fabricantes. • Deverá ser garantido que para alem de serviço de SOC disponível dentro da EU, por questões de alta disponibilidade, o proponente deverá garantir um SOC secundário em pelo menos um outro continente. • Pretende-se que o proponente explique como é constituída a sua equipa de operação e detalhe os diversos perfis que a constituem. • Os analistas deverão possuir certificações governamentais e reconhecidas pelo setor de cibersegurança, CISSP, CISM, Certified Ethical Hacker (CEH), GIAC SANS (GNFA, GCFA, GCIA, GCWN, GCIH, GSNA, GSEC), OSCE, OSCP, CompTIA CSA+, CompTIA CASP+, CSFPC, Cisco Specialist, Cisco CyberOps, SAFe. Para alem destas certificações, deverão ainda ser

		comprovadas certificações de sistemas MCSE, VMWare VCP, Secureworks XDR & VDR, Carbonblack, Cylance, Arcsight, Juniper, McAfee, CSM, Splunk, Citrix, AWS, Microsoft Security. • Por questões de responsabilidade e de atualização técnica contínua, os agentes responsáveis pela monitorização e investigação dos alarmes não poderão ser subcontratados a uma terceira identidade. Deverão fazer parte integral dos quadros técnicos do provedor do serviço MDR. • O proponente deverá eleger um recurso com perfil de "Threat Engagement Manager", que assumirá a interlocução directa com o Município da Nazaré. • Deverá existir um ponto de contacto único das duas partes (gestor de contrato/serviço), por forma a facilitar a comunicação logo desde a fase de adjudicação e implementação do serviço. ➢ *Tecnologia / Plataforma* • Pretende-se um serviço a prestar por plataforma XDR, de analítica de padrões de segurança, reconhecida no mercado à mais de 10 anos, sendo a mesma reconhecida e classificada nos quadrantes mágicos das principais consultoras independentes como a Gartner, Forrester e IDC. • A plataforma a propor como serviço, deverá ter como características principais: • Plataforma "Open" - a solução deverá ser "cloud native", totalmente aberta, que complemente a infraestrutura existente , correlacionando eventos de várias fonte de segurança, fornecendo uma visão geral e abrangente dos diversos ambientes, , protegendo os investimentos anteriores. • Analítica avançada de segurança – capacidade de identificar ameaças anteriormente desconhecidas, eliminar o ruído (falsos positivos) e acelerar as investigações com detetores baseados em knowledge bases reconhecidas no mercado. • Mapeamento MITRE ATT&CK – abranger mais de 90% das táticas e técnicas da framework Mitre ATT&CK. • Defense, Research & Development • Open-source knowledge base • Threat actor system interactions • Adversarial Tactics, Techniques & Common Knowledge



- Automatização das ações de contenção e prevenção – permitir que os analistas do SOC executem a remediação inicial e o isolamento da ameaça, com base nos alertas detetados.
- Inteligência integrada de ameaças – recorrendo a motores e mecanismos de investigação e correlação de padrões.
- Enriquecimento de Alertas – ter um mecanismo que permita tomar ações rápidas e decisivas, adicionando um maior contexto aos alertas recebidos.
- A plataforma deverá possuir mecanismos de deteção de "artificial intelligence" ou "machine learning", beneficiando da inteligência de ameaças e padrões, usando centenas de milhares de pontos de dados compilados entre clientes e serviços, compartilhados em todo o mundo.
- A plataforma deverá conter mecanismos integrados de "Threat Inteligence" (Deep Learning).
- A plataforma deverá fornecer mecanismos de "Threat Hunting", por forma identificar ameaças que possam iludir sistemas automatizados.
- A plataforma deverá detetar e correlacionar ameaças conhecidas e não conhecidas.
- A plataforma deverá suportar investigações colaborativas, com vários agentes e intervenientes
- Deverá permitir a integração com as principais fontes de informação de rede e workloads de cloud (ex: checkpoint, cisto, palo alto, Microsoft, Office 365, VMware, AWS, entre outros).
- Deverá apresentar mecanismos de telemetria, monitorizando e protegendo continuamente o maior número de endpoints (desktops,

		notebooks, instâncias VDI, servidores físicos ou virtuais que corram sistemas operativos Linux, Unix, MacOS ou Windows), devices de rede, workloads de cloud e sistemas de negócio. • A plataforma deverá disponibilizar uma ferramenta de chat, com um especialista de segurança do proponente, sempre que houver necessitade por parte do Município da Nazaré em esclarecer uma dúvida ou tomar uma ação mais imediata. • A plataforma XDR deverá disponibilizar uma consola web, em modelo SaaS, e correspondentes acessos a elementos da equipa de IT do Município da Nazaré, podendo os mesmos visualizar em tempo real, todas as ações e alarmes geridos pelo proponente. • A plataforma XDR deverá disponibilizar APIs (Open Source (GraphQL)), para integração com ambientes de diversos fabricantes de soluções de segurança. ➢ *Processos* • Permitir uma resposta rápida a eventuais ameaças e tempo mínimo de resolução das mesmas. O SLO de investigação para ameaças críticas deverá ser de no máximo 60 Minutos. • O processo de instalação dos agentes EDR nos diversos endpoints, deverá ser incluído no serviço a prestar. • O serviço deverá incluir 40 horas por trimestre, para ajuda na resolução de eventuais vulnerabilidades e remediação remota. • O serviço deverá incluir 40 horas por ano, para apoio na resposta a incidentes/recuperação. • O proponente deverá efetuar uma reunião trimestral com os responsáveis do Município da Nazaré, para revisão do serviço, das incidências ocorridas e/ou melhorias a implementar. • O proponente deverá explicar com o maior detalhe possível, todo o processo de implementação do serviço (setup inicial/onboarding), desde o ponto de vista tecnológico, como dos processos e equipas envolvidas. • O processo de onboarding do serviço deverá contemplar sessões técnicas de recolha de informação. O proponente deverá apresentar uma agenda com os temas a debater nas respetivas sessões técnicas. ➢ *Outros Requisitos* • Os incidentes e alertas deverão ser registados e apresentados em relatórios, consoante a criticidade, e enviados para o um ponto de contacto único. • A plataforma do serviço deverá permitir a exploração e análise de vulnerabilidades Intel.

		• O tratamento de incidentes e inicialização de eventual recuperação de infraestrutura, deverá incluir os seguintes pontos: o Análise de Domain squatting. o Relatórios periódicos e a pedido. o Identificação, investigação e remoção de phishing direcionado. o Tendências dos adversários (análise de táticas, técnicas e procedimentos) o Partilha e implementação de indicadores de compromisso (IOC). o Solicitações ad-hoc para investigações de eventuais ameaças/vulnerabilidades. o Investigação de alertas o Permitir a análise forense de um incidente ➢ *Conteúdo do Serviço* ✓ Estrutura Pretendida para o Serviço • A arquitetura do serviço pretendido deverá ser apresentada em camadas distintas, tendo a capacidade de separar agentes, plataforma de correlação e serviço de SOC (Security Operation Center). O proponente deverá explicar quais os layers do seu serviço. ✓ Monitorização e Alerta de Ameaças O proponente deverá: • monitorizar a infraestrutura on-prem e remota 24/07, existente no Município da Nazaré, quanto a ameaças; • alertar a equipa de IT da Município da Nazaré, sempre que se descubra uma ameaça. • fornecer os primeiros passos para a correção e erradicação da ameaça detetada. • fornecer detalhes das origens dos ataques e gestão inicial de use cases ocorridos. ✓ Análise de Exposição na Web • Pretende-se um serviço inteligente de descoberta de ameaças, monitorizando ativamente múltiplas fontes através da web, ganhando visibilidade do destino dos atacantes, assets, dados e recursos humanos): o Tendências dos atacantes (TTP analysis) o Investigação de alertas o Análise de Domain squatting.

		○ Relatórios periódicos e a pedido. ○ Identificação, investigação e remoção de phishing direcionado. ○ Tendências dos adversários (análise de táticas, técnicas e procedimentos) ○ Partilha e implementação de indicadores de compromisso (IOC). ○ Solicitações ad-hoc para investigações de eventuais ameaças/vulnerabilidades. ✓ <u>Managed Endpoint Detection & Response</u> • O proponente deverá projetar, implementar e gerir a plataforma EDR, por forma a prevenir, detectar e responder proativamente a ameaças nos ambientes endpoints. Deste modo, o proponente deverá conhecer as principais plataformas de Endpoint Protection, Detection and Response (EDR), para fornecer um serviço de gestão de segurança end-to-end. Os serviços de gestão de EDR deverão incluir as seguintes componentes: ○ Análise contínua 24x7, de eventos e alertas de segurança nos endpoints. ○ Proteção total contra exploits, malware, fileless attacks, etc. ○ Políticas altamente personalizáveis e definidas pelo utilizador. ○ Visualização intuitiva de ataques aos endpoints. ○ Detecção proativa, alinhada com a matriz Mitre ATT&CK. ○ Agentes de endpoints autónomos e não intrusivos. ✓ <u>Gestão de Vulnerabilidades</u> • O proponente deverá providenciar uma aproximação holística, para gestão de vulnerabilidades e riscos críticos, na resolução de eventuais falhas detetadas. • Deverá utilizar processos automáticos para a identificação de falhas, análises de impacto e prevenção de incidentes críticos. • A gestão de vulnerabilidades por parte do proponente, deverá incluir: ○ Priorização de vulnerabilidades ○ Remediação e mitigação especializadas ○ Análise preditiva ○ Verificação de vulnerabilidades ○ Simulação de testes

		✓ Resposta e Resolução de um Incidente • O proponente deverá ilustrar e explicar todo o processo de workflow, na ocorrência de um incidente. Deverá especificar quais os workflows e equipas envolvidas na resposta resolução a incidentes, mencionar os processos, procedimentos e meios de comunicação utilizados, e ainda mencionar quando existam custos adicionais a serem aplicados ao serviço base (time & materials, se aplicável). ✓ Serviços On-Call para Resposta a Incidentes e Análise Forense • Embora não sendo alvo desta consulta, nem devendo estar incluído na proposta financeira, o proponente deverá explicar quais os seus serviços recuperação das infraestruturas/ dados afetados. • O serviço deverá possuir disponibilidade de equipa multi-tecnologia, de resposta e remediação de incidentes e deverá explicar o processo de aticvação dessa equipa, caso seja necessário e contratado adicionalmente. • Como cenário hipotético para o Município da Nazaré, e em caso de uma catástrofe de criticidade máxima, o proponente deverá responder no máximo até 2 horas, para iniciar remotamente o plano de recuperação. Quando necessário e se assim se justificar, o proponente deverá fornecer um especialista onsite, no intervalo máximo de 48 horas, após a ocorrência do ataque, sempre que contratado adicionalmente pelo Município da Nazaré. • Em qualquer caso, o serviço alvo desta consulta, deverá fornecer as competências necessárias para realizar remotamente as atividades e tarefas iniciais de resposta imediata e remediação de incidentes. • O proponente deverá ainda possuir competências, metodologia e mecanismos para efetuar uma análise forense de um determinado ataque, mas suas diversas componentes: o Análise forense de endpoints o Análise forense de dispositivos móveis o Análise forense da rede o Análise forense de workloads de Cloud ✓ Modelo Financeiro • Pretende-se nesta consulta que a valorização dos serviços solicitados seja apresentada com base nas premissas seguintes: o Contrato com a duração mínima de 3 ano(s).

		o Apresentação de um custo único por dispositivo protegido (incluindo postos de trabalho, máquinas virtuais, devices de rede, Office 365 e workloads de cloud). o O custo do serviço não deverá depender do número de logs a analisar, eventos, mensagens e/ou incidentes analisados por segundo (EPS/MPS). Será da responsabilidade do prestador ter a capacidade técnica de suportar todos os eventos necessários e a posterior análise dos mesmos. Não deverão ser imputados custos adicionais pelo aumento de logs diários. o O serviço proposto deverá permitir a análise de um número infinito de logs, sem custos adicionais. o Os eventos gerados pelos equipamentos de rede (como firewalls, IDS, IPS), bem como os workloads de cloud e eventos Office 365 deverão ser integrados na plataforma XDR, e analisados sem haver um limite máximo ou custos adicionais, para além dos custos inerentes aos endpoints subscritos. o Para além do custo por dispositivo, o serviço não deverá apresentar custos adicionais de setup ou de assessment e análise de vulnerabilidades. o Todo o licenciamento de plataformas e ferramentas de segurança necessárias à prestação do serviço, deverão estar incluídas no custo a apresentar por dispositivo. o Caso não existam instalados agentes EDR, compatíveis e de integração direta com a plataforma XDR proposta, o proponente deverá disponibilizar um agente EDR sem custos adicionais (incluído no serviço), que deverá integrar automaticamente com a plataforma proposta, por forma a tirar partido dos motores de telemetria e de correlação da plataforma XDR.

SERVIÇOS

No âmbito do presente descritivo técnico, estão incluídos os seguintes serviços:

Qtd	Equipamento	Configuração
		SERVIÇOS
1	Serviço de instalação, configuração e implementação	***Planeamento:*** • Planeamento de Projeto e elaboração do Cronograma; • Levantamento de Requisitos e condições técnicas/logísticas para a execução do projeto; • Levantamento de Pré-Instalação; • Aprovação e Calendarização; ***Montagem dos Equipamentos:*** • Desembalagem e conferência de todo o fornecimento; • Montagem e Instalação de todos os equipamentos; • Ligações dos equipamentos (Cabos de rede, Fibra e cabos de energia); • Upgrade de Firmware (caso necessário); • Testes e Operacionalidade; ***Armazenamento:*** • Criação de volumes/ Movimentação de volumes; • Apresentação de volumes aos novos servidor; • Implementação de todas as funcionalidades disponíveis da solução de armazenamento (Thin Provisioning, Auto Tiering etc.) • Configuração de replicação de bloco e ficheiro entre as matrizes de armazenamento propostas. • Configuração de replicação de bloco entre a matrizes de armazenamento proposta para produção e matriz de armazenamento atualmente em produção e que transitará para o site de DR. **Nota específica**: O Município da Nazaré providenciará os meios de transmissão necessários para as rotinas de replicação. Assim sendo, meramente por questões de operacionalidade, a replicação direta entre as matrizes de armazenamento novas propostas poderá ter que ser operacionalizada em período posterior, mas nunca superior a 4 meses.

		Serviços de Implementação/Migração da Plataforma de Virtualização: • Verificação de Requisitos • Preparação, Instalação e Configuração do Software de Virtualização de Servidores; • Criação de Servidores Windows e/ou Linux virtuais; • Balanceamento do ambiente de virtualização para o novo servidor; • Configuração do serviço de alta disponibilidade e consola de administração; • Importação de todas as VMs atualmente em produção para a nova estrutura a implementar. ***Serviços de Implementação da Plataforma de Backup, Recuperação de Desastre e Continuidade de Negócio:*** • Verificação de Requisitos; • Preparação, Instalação e Configuração do Software de Backup, Recuperação de Desastre e Continuidade de Negócio; • Inicio de proteção de todos os Servidores Windows e/ou Linux, virtuais; • Configuração do serviço de Deduplicação, Compressão e Encriptação; • Configuração dos serviços de replicação e recuperação remota; • Configuração do serviço de recuperação instantânea; • Configuração do serviço de Recuperação Universal; • Configuração do serviço de Consola de gestão e alertas; • Configuração do serviço de dispositivos para repositório dos backups; • Configuração do serviço de políticas de retenção; • Configuração do serviço de pontos de restauro (RPO) e tempos de restauro (RTO); • Testes e Operacionalidade; ***Serviços de configuração de rede:*** Configuração switch FC/ ToR, herdando todas as configurações existentes e respeitando as boas práticas de interligação e configuração no que concerne alta disponibilidade, integrando com os equipamentos de rede existentes;

		Serviços de cyber segurança, deteção e resposta: Configuração de toda a plataforma; ***Formação:*** Deverá estar incluída formação "on-the-job"; ***Suporte pós-venda adicional:*** Deverão ser contempladas no mínimo 100 horas de suporte pós-venda para operações diversas; ***Relatório:*** Relatório detalhado de Implementação global da solução;

CONCURSO PÚBLICO

Artigo 20.º n. º1 alínea b) do Código dos Contratos Públicos

PROGRAMA DO CONCURSO

Aquisição de Bens – Servidor Informático (*Datacenter*)

PARTE I

CLÁUSULAS JURÍDICAS

CAPITULO 1

DISPOSIÇÕES GERAIS

ARTIGO 1º

OBJETO DO CONCURSO

O presente concurso público, nos termos do artigo 20º, n.º 1, alínea b) do Código dos Contratos Públicos (adiante CCP), tem por objeto a Aquisição de Bens – Servidor Informático (*Datacenter*).

ARTIGO 2º

ENTIDADE PÚBLICA CONTRATANTE

1. Município de Nazaré, NIPC 507 012 100, sedeado no Edifício dos Paços do Concelho, na Avenida Vieira Guimarães, n.º 54 (CP 2450-112), Nazaré, com o endereço telefónico 00351 262 550 010, endereço eletrónico geral@cm-nazare.pt e endereço de plataforma eletrónica de contratação pública www.vortal.biz.
2. O órgão que tomou a decisão de contratar foi a Câmara Municipal da Nazaré.

ARTIGO 3º

CONCORRENTES

1. Podem apresentar propostas as pessoas singulares ou coletivas que não se encontrem em nenhuma das situações referidas no artigo 55º, do Código dos Contratos Públicos.
2. Não é permitida a apresentação de propostas por um agrupamento de concorrentes.

ARTIG0 4º

CRITÉRIO DE ADJUDICAÇÃO

A adjudicação é feita segundo o critério da proposta economicamente mais vantajosa, na modalidade de avaliação do preço mais baixo, de acordo com o artigo 74.º, n.º 1, alínea b), do CCP.

ARTIGO 5º

CONDIÇÕES DE PAGAMENTO

Nas condições de pagamento a apresentar pelos concorrentes não podem ser propostos adiantamentos por conta dos bens a fornecer.

SECÇÃO I

PROPOSTAS

ARTIGO 6º

APRESENTAÇÃO E ABERTURA DE PROPOSTAS

1. As propostas e os documentos que as acompanham devem ser apresentadas até às 23:59 horas do 6.º dia, a contar da data de publicação do anúncio no Diário da República.
2. As propostas e os documentos que as acompanham devem ser apresentadas diretamente em plataforma eletrónica, www.vortal.biz, nos termos do artigo 62.º, do CCP.
3. A data limite fixada no n.º 1 pode, a pedido de qualquer interessado e em casos devidamente fundamentados, ser prorrogada por prazo considerado adequado, sem prejuízo do disposto no artigo 64.º, n.ºs 1e 2, do CCP.
4. A prorrogação de prazo prevista no número anterior beneficia todos os interessados.
5. O júri procede à abertura das propostas às 09h00 do dia útil seguinte à data limite para entrega das propostas.

ARTIGO 7º

FORNECIMENTO DAS PEÇAS DO PROCEDIMENTO

1. As peças do procedimento encontram-se disponíveis na plataforma eletrónica www.vortal.biz.
2. O processo encontra-se patente nas Relações Públicas, do Município de Nazaré, sedeado no Edifício dos Paços do Município, na Avenida Vieira Guimarães, n.º 54 (CP 2450-112), Nazaré, onde pode ser examinado todos os dias úteis das 09:00h às 12:30h e das 14:00h às 16:00h.

ARTIGO 8º

ESCLARECIMENTOS, RETIFICAÇÃO E ALTERAÇÃO DAS PEÇAS DO PROCEDIMENTO

1. Os esclarecimentos, retificação e alteração das peças do procedimento regem-se pelo disposto no artigo 50.º, do Código dos Contratos Públicos.
2. O órgão competente para prestar esclarecimentos é o júri designado para conduzir o procedimento.

ARTIG0 9º

PREÇO ANORMALMENTE BAIXO

Fixando, nos termos do n. º2 do artigo 71.º do CCP, "(...) a entidade adjudicante deve fundamentar a necessidade de fixação do preço ou do custo anormalmente baixo, bem como os critérios que presidiram a essa fixação, designadamente os preços médios obtidos na consulta preliminar ao mercado, se tiver existido".

ARTIGO 10º

PROPOSTA

1. Na proposta o concorrente manifesta a sua vontade de contratar e indica o modo pelo qual se dispõe a fazê-lo.
2. A proposta é constituída pelos seguintes documentos:

a) Declaração do concorrente de aceitação do conteúdo do caderno de encargos, elaborada em conformidade como modelo constante do Anexo I ao presente Programa de Procedimento;

b) Proposta de Preço, elaborada em conformidade como modelo constante do Anexo II ao presente Programa de Procedimento;

c) Certidão Permanente ou Código de Acesso (no caso de empresa), ou Certidão de Início de Atividade (no caso pessoa em nome individual)

d) Nota Justificativa de Preço Proposto

3. O preço da proposta é indicado em algarismos e não inclui o IVA.
4. A proposta deve mencionar expressamente que ao preço total acresce o IVA, indicando-se o respetivo valor e a taxa legal aplicável.
5. Sob pena de exclusão todos os documentos que constituem a proposta, submetidos na plataforma eletrónica (www.vortal.biz), são obrigatoriamente redigidos em português e têm de ser individualmente assinados mediante a utilização de certificado de assinatura eletrónica qualificada, nos termos dos artigos 54.º e 68.º da Lei 96/2015, de 17 de agosto. No caso em que a assinatura eletrónica certificada não possa relacionar diretamente o assinante com o concorrente é obrigatória a apresentação de documento comprovativo de poderes de representação.
6. O concorrente fica obrigado a manter a sua proposta durante um período de 66 dias contados do termo do prazo fixado para a apresentação das propostas.
7. Não são admitidas propostas relativas a parte do serviço que se pretende contratualizar.

ARTIGO 11º

PROPOSTAS COM VARIANTES

1. Não é admitida a apresentação de propostas com variantes.
2. Para efeitos do presente concurso, proposta com variantes é aquela que relativamente a um ou mais aspetos da execução do contrato a celebrar, contenha atributos que digam respeito a condições contratuais alternativas.

SECÇÃO II

ADJUDICAÇÃO

ARTIGO 12º

ESCOLHA DO ADJUDICATÁRIO

Depois de cumpridas as formalidades previstas no CCP, a entidade competente para autorizar a despesa, com base num relatório fundamentado elaborado pelo Júri, escolhe o adjudicatário.

ARTIGO 13º

NOTIFICAÇÃO DA ADJUDICAÇÃO

Nos cinco dias úteis posteriores à respetiva decisão de adjudicação referida no artigo anterior, todos os concorrentes são notificados do ato de adjudicação, através da plataforma eletrónica www.vortal.biz.

ARTIGO 14º

ANULAÇÃO DA ADJUDICAÇÃO

1. A adjudicação caduca-se, por facto que lhe seja imputável, o adjudicatário, não apresentar os documentos de habilitação:
   a) No prazo fixado neste programa de procedimento;
   b) No prazo fixado pelo órgão competente para a decisão de contratar, no caso previsto no n.º 8, do artigo 81º, do CCP;
   c) Redigidos em língua portuguesa ou acompanhados de tradução devidamente legalizada.
2. Nos casos previstos no número anterior, o órgão competente para a decisão de contratar deve adjudicar a proposta ordenada em lugar subsequente.
3. Constituem também causas de caducidade da adjudicação as indicadas no artigo 87.º A e no artigo 91.º, n.º 1, ambos do CCP.

ARTIGO 15º

CAUSAS DE NÃO ADJUDICAÇÃO

Não há lugar à adjudicação nas hipóteses enumeradas no artigo 79º, n.º 1, do CCP.

SECÇÃO III

CONTRATO

ARTIGO 16º

DOCUMENTOS DE HABILITAÇÃO

1. O adjudicatário deve apresentar os seguintes documentos de habilitação, no prazo de 5 dias úteis, contados da data de notificação da adjudicação:
   a) Declaração emitida conforme modelo constante do Anexo II, ao presente Programa de Procedimento;
   b) Declaração de Situação regularizada referente a contribuições para a Segurança Social;
   c) Declaração de Situação regularizada referente a impostos devidos ao Estado Português;
   d) Certificado de Registo Criminal dos titulares dos órgãos sociais de administração, direção ou gerência que se encontrem em efetividade de funções;
2. A apresentação dos documentos de habilitação rege-se pelo disposto nos artigos 81º e seguintes, do CCP.
3. As irregularidades detetadas nos documentos de habilitação devem ser supridas no prazo de três dias úteis, a contar da respetiva notificação, sob pena de a adjudicação caducar.

ARTIGO 17º

ACEITAÇÃO DA MINUTA DO CONTRATO

1. A minuta do contrato é enviada, para aceitação, ao adjudicatário.
2. A minuta considera-se aceite pelo adjudicatário quando haja aceitação expressa ou quando não haja reclamação nos cinco dias úteis subsequentes à respetiva notificação.

ARTIGO 18º

RECLAMAÇÕES CONTRA A MINUTA

1. São admissíveis reclamações contra a minuta quando dela constem obrigações que contrariem ou que não constem dos documentos que integram o contrato.
2. Em caso de reclamação, a entidade que aprova a minuta notifica o adjudicatário da sua decisão, equivalendo o silêncio à rejeição da reclamação.

ARTIGO 19º

OUTORGA DO CONTRATO ESCRITO

1. O contrato deve ser celebrado no prazo de 30 dias úteis contados da data da aceitação da minuta ou da decisão sobre a reclamação, nos termos do artigo 104º, n.º 1, do CCP.
2. A entidade pública contratante comunica ao adjudicatário, com a antecedência mínima de cinco dias úteis, a data, hora e local em que ocorrerá a outorga do contrato.
3. A adjudicação caduca-se, por facto que lhe seja imputável, o adjudicatário não comparecer no dia, hora e local fixados para a outorga do contrato.
4. Se, por facto que lhe seja imputável, a entidade adjudicante não outorgar o contrato no prazo previsto no n.º 1, o adjudicatário pode desvincular-se da proposta.

SECÇÃO IV

DISPOSIÇÕES FINAIS

ARTIGO 20º

FALSIDADE DE DOCUMENTOS E DE DECLARAÇÕES

Sem prejuízo da participação à entidade competente para efeitos de procedimento criminal, a falsificação de qualquer documento de habilitação ou a prestação culposa de falsas declarações determina a caducidade da adjudicação, sendo aplicável o disposto no artigo 86º, n.º 3, do CCP.

ARTIGO 21º

CAUÇÃO PARA GARANTIR O CUMPRIMENTO DE OBRIGAÇÕES

Não é exigida a apresentação de caução, nos termos do artigo 88º, n.º 2, do CCP.

ARTIG0 22º

CADUCIDADE DA ADJUDICAÇÃO

1. A adjudicação caduca se, por facto que lhe seja imputável, o adjudicatário, não apresentar os documentos de habilitação:
   a) No prazo fixado neste programa de procedimento;
   b) No prazo fixado pelo órgão competente para a decisão de contratar, no caso previsto no n.º 8, do artigo 81º, do CCP;
   c) Redigidos em língua portuguesa ou acompanhados de tradução devidamente legalizada.
2. Nos casos previstos no número anterior, o órgão competente para a decisão de contratar deve adjudicar a proposta ordenada em lugar subsequente.
3. Constituem também causas de caducidade da adjudicação as indicadas no artigo 87.º-A e no artigo 91.º, n.º 1, ambos do CCP.

ARTIGO 23º

PREÇO BASE

O preço total máximo que a entidade adjudicante se dispõe a pagar pela totalidade do objeto do contrato é 197.600,00 euros, ao qual acresce o IVA à taxa legal em vigor.

ARTIG0 24º

CRITÉRIO DE DESEMPATE

1. Em caso de empate no valor das propostas admitidas, far-se-á o desempate por sorteio, realizado pelo júri na presença de um representante de cada um dos concorrentes, do qual

será redigida ata a assinar por todos os intervenientes.

2. Para efeitos do número anterior, todos os concorrentes serão notificados da data, hora e local do sorteio com a antecedência de 3 dias seguidos.
3. Os concorrentes deverão apresentar-se munidos da respetiva identificação e de comprovativo ou declaração que confira poderes para representar a entidade, emitida por quem tem poderes para a obrigar.
4. No caso de não estarem presentes todos os representantes, o júri procede à realização do sorteio, com os concorrentes presentes na data, hora e local marcados.

ARTIGO 25º

ENCARGOS DOS CONCORRENTES

Constituem encargos dos concorrentes todas as despesas inerentes à elaboração das propostas.

ARTIGO 26º

COMUNICAÇÕES E NOTIFICAÇÕES

As notificações previstas no Código dos Contratos Públicos no desenrolar do presente procedimento serão efetuadas nos termos do artigo 61.º, da Lei n.º 96/2015, de 17 de agosto.

ARTIGO 27º

LEGISLAÇÃO APLICÁVEL

A tudo o que não esteja especialmente previsto no presente programa aplica-se o regime previsto no Código dos Contratos Públicos e respetiva regulamentação.

Com os meus melhores cumprimentos,

Ricardo Pereira

Enterprise Solutions Manager

Espectro | Sistemas de Informação SA

Mobile +351 96 325 95 68

Chamada para rede móvel nacional

ricardo@espectro.pt

Rua Dr. Luís A. Duarte Santos, N20, 3030-403 Coimbra

Ed. Infante, Av. D. João II, N35, Piso 11 A/D, Parque das Nações, 1990-083 Lisboa

Portugal

Dell EMC Partner | Platinum

--

Tiago Grilo Santos
Especialista de Informática
Gabinete de Tecnologias de Informação e Multimédia
Município da Nazaré | Câmara Municipal
Av. Vieira Guimarães nº54, 2450 - 951 Nazaré
Tlm.: +351 911 070 507 | Tel: +351 262 560 010
cm-nazare.pt

Anexos:

- image001.png
- image002.jpg
- image003.jpg

Fwd: Espectro SA - Projeto Datacenter + XDR
03/04/2023 18:47

De: "Tiago Grilo Santos" <tiago.santos@cm-nazare.pt>
Para: Aproviosionamento <sac@cm-nazare.pt>

---------- Mensagem encaminhada ---------
From: **Walter Chicharro** <walter.chicharro@cm-nazare.pt>
Data: seg., 3/04/2023 às 18:42
Assunto: Re: Espectro SA - Projeto Datacenter + XDR
Para: Tiago Grilo Santos <tiago.santos@cm-nazare.pt>

autorizo

Walter Chicharro, Dr.
Presidente da Câmara Municipal da Nazaré

NAZARÉ

Sofia Carepa, Dra. - Secretária
Tel.: 262 550 017
Av. Vieira Guimarães nº54, 2450 - 951 Nazaré
Tel: +351 262 550 010
cm-nazare.pt

De: Tiago Santos <tiago.santos@cm-nazare.pt>
Data: terça-feira, 28 de março de 2023, 17:34
Para: Walter Chicharro <walter.chicharro@cm-nazare.pt>
Assunto: Fwd: Espectro SA - Projeto Datacenter + XDR

Viva Sr. Presidente, Boa tarde,

Conforme já largamente debatido, segue em anexo um orçamento para remodelação do nosso datacenter.

Melhores cumprimentos

Tiago Grilo Santos
Especialista de Informática
Gabinete de Tecnologias de Informação e Multimédia
Município da Nazaré | Câmara Municipal
Av. Vieira Guimarães nº54, 2450 - 951 Nazaré
Tlm.: +351 911 070 507 | Tel: +351 262 550 010
cm-nazare.pt

---------- Forwarded message ---------
De: **Ricardo Pereira** <ricardo@espectro.pt>
Date: terça, 28/03/2023 à(s) 15:08
Subject: Espectro SA - Projeto Datacenter + XDR
To: Tiago Grilo Santos <tiago.santos@cm-nazare.pt>

Viva Tiago,

Conforme combinado, em anexo segue proposta.

Ligo de seguida.

Obrigado.