

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

AQUISIÇÃO DE SERVIÇOS DE DESENVOLVIMENTO E INFRAESTRUTURA TECNOLÓGICA PARA O PROJETO @MADEIRA

PROCESSO N.º DRI-24/CP/2022

CADERNO DE ENCARGOS

DRI-900.20.001-2.2/2



1/68

Azinhaga do Poço Barral, n.º 23, Edifício Funchal Business Center, piso 1 | 9000-638 Funchal
T. +351 291 145 190 | www.madeira.gov.pt | dri@madeira.gov.pt | NIF: 671 001 310 | NISS: 200 0498 1685



REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Índice

PARTE I – DISPOSIÇÕES INICIAIS	6
Cláusula 1. ^a	6
Conteúdo funcional do objeto.....	6
Cláusula 2. ^a	7
Preço Base	7
Cláusula 3. ^a	7
Local de Entrega dos Bens	7
PARTE II – DISPOSIÇÕES GERAIS.....	8
Cláusula 4. ^a	8
Patentes, Licenças e Marcas Registadas	8
Cláusula 5. ^a	8
Sigilo	8
PARTE III – OBRIGAÇÕES CONTRATUAIS	10
SECÇÃO I – OBRIGAÇÕES DO FORNECEDOR	10
Cláusula 6. ^a	10
Obrigações Principais do Fornecedor	10
Cláusula 7. ^a	10
Prazo de fornecimento, instalação e configuração	10
Cláusula 8. ^a	11
Aceitação.....	11
Cláusula 9. ^a	11
Propriedade.....	11
Cláusula 10. ^a	11
Conformidade e garantia técnica.....	11
Cláusula 11. ^a	11
Procedimentos ambientais e de gestão de resíduos	11
Cláusula 12. ^a	11
Responsabilidade	11
Cláusula 13. ^a	12
Dever de boa execução.....	12
SECÇÃO II – OBRIGAÇÕES DA ENTIDADE ADJUDICANTE.....	12
Cláusula 14. ^a	12
Preço contratual e formas de pagamento.....	12
Cláusula 15. ^a	13
Condições de pagamento	13
Cláusula 16. ^a	13
Deduções nos pagamentos.....	13





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Cláusula 17. ^a	13
Designação de Gestor	13
PARTE IV – PENALIDADES CONTRATUAIS E RESOLUÇÃO	14
Cláusula 18. ^a	14
Penalidades contratuais	14
Cláusula 19. ^a	14
Força maior	14
Cláusula 20. ^a	15
Resolução do contrato	15
RESOLUÇÃO DE LITÍGIOS	16
Cláusula 21. ^a	16
Foro competente	16
PARTE V – DISPOSIÇÕES FINAIS	17
Cláusula 22. ^a	17
Comunicações e notificações	17
Cláusula 23. ^a	17
Produção de efeitos	17
Cláusula 24. ^a	17
Contagem dos Prazos	17
Cláusula 25. ^a	17
Legislação aplicável	17
PARTE VI	18
SECÇÃO I – ESPECIFICAÇÕES TÉCNICAS E FUNCIONAIS	18
Cláusula 26. ^a	18
Arquitetura geral	18
Cláusula 27. ^a	18
Diagrama da Infraestrutura Tecnológica	18
SECÇÃO II – INFRAESTRUTURAS TECNOLÓGICAS	19
Cláusula 28. ^a	19
Requisitos da Componente de Processamento e Computação	19
Requisitos Técnicos	20
Características físicas e crescimento	21
Administração	22
Gestão	22
Atualização/manutenção	23
Cláusula 29. ^a	26
Requisitos da Componente de Armazenamento	26
Requisitos da Solução de Armazenamento	26

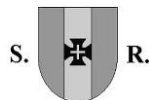




REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Requisitos genéricos	27
Requisitos relativos a capacidade e especificações técnicas	30
Cláusula 30.^a	30
Requisitos da Componente de Rede e Comunicações LAN	30
Cláusula 31.^a	30
Requisitos da Componente de Proteção de Dados	30
Descrição da Infraestrutura a Proteger	32
Integrações e suportabilidades	34
Cláusula 32.^a	34
Requisitos da Componente de Ciber-Resiliência	34
Cláusula 33.^a	35
Requisitos da Componente de Segurança de Perímetro	35
Especificações técnicas da Solução de Firewall	35
Hardware (obrigatório dentro do mesmo equipamento):	36
Sandboxing:	41
IOT Security:	42
Data Loss Prevention:	43
SD-WAN:	44
Relatórios & Logs:	44
Outras Funcionalidades:	45
Mapa de Quantidades:	46
SECÇÃO III – DESENVOLVIMENTO APLICACIONAL DA PLATAFORMA @MADEIRA	47
Cláusula 34.^a	47
Requisitos da Componente de Desenvolvimento Aplicacional	47
1. Enquadramento	47
2. Requisitos da Plataforma Aplicacional @MADEIRA – Módulo Apoio à Atividade Comercial	48
3. Requisitos da Plataforma Aplicacional @MADEIRA – Módulo de Visitas Virtuais	52
4. Arquitetura de Referência	55
5. Modelo de Gestão do Projeto	56
SECÇÃO IV – REQUISITOS PARA A PRESTAÇÃO DE SERVIÇOS	57
Cláusula 35.^a	57
Requisitos da Componente de Serviços de Suporte e Manutenção	57
Cláusula 36.^a	58
Requisitos da Componente de Serviços de Instalação, Configuração e Formação	58
Cláusula 37.^a	59
Requisitos da Componente de Serviços de Desenvolvimento e Suporte Aplicacional	59
Local de Prestação do Serviço e Constituição da Equipa	59

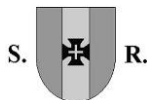




REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Requisitos dos Serviços de Manutenção Corretiva e Preventiva	62
Cláusula 38.^a	64
Requisitos da Componente de Serviços de Administração de sistemas	64
Cláusula 39.^a	65
Requisitos da Componente de Alojamento e Comunicações	65
ANEXO I – CONSULTA PRELIMINAR AO MERCADO	67





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

PARTE I – DISPOSIÇÕES INICIAIS

Cláusula 1.^a

Conteúdo funcional do objeto

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar pela Região Autónoma da Madeira, na sequência do procedimento pré-contratual que tem por objeto a “Aquisição de serviços de desenvolvimento e infraestrutura tecnológica para o projeto @MADEIRA.”
2. Enquadramento geral:

O projeto @MADEIRA irá criar na Região Autónoma da Madeira uma estratégia de transição digital única para as empresas regionais, qualificando-as como “empresas digitais”, não só numa perspetiva promocional, mas ativando processos operacionais inovadores e decisivos para a sua competitividade, quer ao nível do comércio eletrónico, cibersegurança, interação com os seus clientes e capacidade de concorrerem globalmente.

Através deste projeto, a Região Autónoma da Madeira pretende concretizar um conjunto de objetivos:

- a) Estabelecer através da Transição Digital uma maior proximidade do Governo com a população e com os Agentes Económicos da região;
- b) Alcançar maior agilidade e rapidez na disponibilização de novos serviços;
- c) Promover a integração de serviços e mobilidade no acesso;
- d) Promover o cumprimento das Diretivas Comunitárias e Nacionais de Proteção de Dados;
- e) Promover a qualificação nas novas competências digitais;
- f) Realizar a Transformação Digital do processo comercial, criando novos canais entre os operadores, turistas e Administração Regional;
- g) Enriquecer a experiência do Turista na sua visita à Região, disponibilizando um Guia Digital que o apoiará e guiará em toda a sua estadia;
- h) Promover a Madeira como região turística de grande beleza natural e patrimonial;
- i) Através de novas tecnologias, nomeadamente com a utilização de algoritmos de Inteligência Artificial, adequar a oferta Turística e Comercial da Região ao perfil do Turista, transformando a estadia numa experiência personalizada;
- j) Catalogar e disponibilizar toda a oferta turística e comercial da região num portal único, criando um veículo de comunicação entre os operadores e a Administração Regional;
- k) Criar um selo de Qualidade e certificação para a oferta turística e comercial da Região, reforçando a credibilidade e confiança nos operadores
- l) Criar sistemas de apoio à decisão que permitam aos operadores e Administração Regional definir estratégias e adequar a sua oferta com vista ao aperfeiçoamento contínuo e melhoria de resultados;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- m) Criar novos canais e processos para a promoção da Região Autónoma da Madeira como destino de excelência, fazendo a divulgação da sua oferta com um alcance global;
3. **Âmbito:**
- O presente procedimento, engloba as componentes necessárias para a implementação do Projeto @MADEIRA, e compreende:
- a) Serviços de Desenvolvimento Aplicacional da Solução de Suporte ao Projeto @MADEIRA;
 - b) Infraestrutura de Comunicações, Cibersegurança, Processamento, Armazenamento e Proteção de Dados necessários para a exploração contínua da Solução;
 - c) Licenciamento de todo o software base necessário para a correta exploração da solução nas vertentes de Comunicações, Cibersegurança, Processamento, Armazenamento e Proteção de Dados;
 - d) Serviços de Implementação, Suporte, Desenvolvimento Aplicacional e Formação necessários para o correto desenvolvimento e exploração da solução;
 - e) Serviços de Acompanhamento e Apoio durante o período de 2 (dois) anos após a entrada em produção da solução.

Cláusula 2.^a

Preço Base

1. O preço máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o objeto do contrato é de € 3.500,000.00 (Três Milhões e Quinhentos mil Euros), a que acresce IVA à taxa legal em vigor.
2. O preço base foi estipulado com recurso a uma consulta preliminar ao mercado, fazendo uso do disposto no artigo 35.º-A do CCP, sendo que, para efeitos de cumprimento do disposto no n.º 4 do mesmo artigo, todas as informações pertinentes trocadas no âmbito da participação do concorrente na preparação do procedimento de formação do contrato, encontram-se exaradas no Anexo I ao presente caderno de encargos.

Cláusula 3.^a

Local de Entrega dos Bens

O local de entrega, instalação e configuração dos bens objeto do contrato a celebrar será em local a designar na Ilha da Madeira.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

PARTE II – DISPOSIÇÕES GERAIS

Cláusula 4.^a

Patentes, Licenças e Marcas Registadas

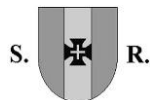
1. Os contraentes garantem que respeitam as normas relativas à propriedade intelectual e industrial, designadamente, direitos de autor, licenças, patentes e marcas registadas, relacionadas com o hardware, software e documentação técnica que utilizam no desenvolvimento da sua atividade.
2. A Direção Regional de Informática não assume qualquer responsabilidade por infrações cometidas pelo fornecedor, no âmbito da execução do contrato, relativamente a direitos de propriedade intelectual e industrial relacionados com o hardware, software e documentação técnica por este utilizado, cujos direitos e autorizações legais para o efeito devam por ele ser assegurados.

Cláusula 5.^a

Sigilo

1. Os Contraentes obrigam-se a garantir o sigilo quanto a informação diretamente relacionada com o objeto do presente contrato, bem como, tomar todas as medidas necessárias para que os seus funcionários e agentes se vinculem a igual obrigação, quanto aos conhecimentos que venham a ter no âmbito dos trabalhos em que estão envolvidos.
2. Os Contraentes tratarão como confidencial toda a informação por eles devidamente identificada como tal, ou que, pela natureza das circunstâncias que rodeiam a sua divulgação deva, em boa-fé, ser considerada como confidencial.
3. Para efeitos do disposto no número anterior, considera-se como confidencial, independentemente da sua identificação como tal, toda a informação a que o fornecedor tenha acesso relacionada com sistemas de segurança para proteção de informação, sistemas informáticos, sistemas de informação, instalações, métodos de trabalhos e core business da Região Autónoma da Madeira
4. Carece de consentimento prévio, a prestar pela Direção Regional de Informática:
 - a) A divulgação pelo fornecedor de qualquer informação, sob qualquer forma, relacionada com o presente projeto ou com qualquer outro de que venha a ter conhecimento;
 - b) A utilização do logótipo da Direção Regional de Informática ou da Região Autónoma da Madeira para efeitos de publicidade, assim como a referência à sua qualidade de fornecedor.
5. Encontra-se excluída da presente obrigação de confidencialidade a informação que:
 - a) Tenha sido prévia e legitimamente divulgada por terceiros a qualquer um dos contraentes;
 - b) Se encontre disponível para o público em geral;
 - c) Os contraentes tenham sido legal ou judicialmente obrigados a revelar, desde que observados os procedimentos estabelecidos para o efeito;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- d) Seja conhecida do contraente que a revelou em momento anterior à celebração do presente contrato;
- e) Tenha sido transmitida ao contraente por uma terceira entidade sem que lhe tenha sido imposta qualquer obrigação de confidencialidade;
- f) Os contraentes acordem, por escrito, na possibilidade da sua divulgação.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

PARTE III – OBRIGAÇÕES CONTRATUAIS

SECÇÃO I – Obrigações do Fornecedor

Cláusula 6.^a

Obrigações Principais do Fornecedor

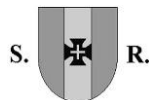
1. Sem prejuízo de outras obrigações previstas na legislação aplicável na celebração do contrato, decorrem para o fornecedor as seguintes obrigações principais:
 - a) Obrigação de fornecer os bens e prestar os serviços identificados na sua proposta;
 - b) Obrigação de garantia do resultado.
2. A título acessório, o fornecedor fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à execução do contrato, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Cláusula 7.^a

Prazo de fornecimento, instalação e configuração

1. O adjudicatário obriga-se a:
 - a) Entregar, instalar e configurar os bens, com todos os elementos referidos no presente Caderno de Encargos, no prazo máximo de 240 (duzentos e quarenta) dias, contados da data de entrada em vigor do contrato.
 - b) O prazo referido na alínea anterior deverá obedecer ao seguinte planeamento:
 - Prazo para Implementação da Infraestrutura Tecnológica: 120 (cento e vinte) dias após assinatura do Contrato.
 - Desenvolvimento do Módulo Aplicacional @Madeira – Módulo de Apoio à Atividade Comercial: 180 (cento e oitenta) dias após assinatura do contrato.
 - Desenvolvimento do Módulo Aplicacional @Madeira – Módulo de Visitas Virtuais: 240 (duzentos e quarenta) dias após assinatura do contrato.
 - c) Dar formação com um mínimo de 16 (dezassexes) horas a uma equipa composta por até 4 (quatro) pessoas a indicar pela entidade adjudicante necessária para o correto desenvolvimento e exploração da solução; os conteúdos da ação de formação encontram-se descritos na Cláusula 36.^a do presente Caderno de Encargos;
 - d) Manter e assegurar o integral funcionamento dos bens e serviços objeto do contrato, incluindo o funcionamento da aplicação, pelo prazo de 36 (trinta e seis) meses contados da data da sua entrada em vigor.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Cláusula 8.^a

Aceitação

1. Após a entrega, instalação e configuração dos bens, a Direção Regional de Informática lavrará, no prazo máximo de 5 (cinco) dias úteis, um auto de aceitação, que será precedido de realização de testes, onde ficará registada a data de aceitação dos mesmos.
2. O auto de aceitação será enviado ao adjudicatário.
3. Não é permitida a aceitação tácita dos bens e serviços objeto do contrato.

Cláusula 9.^a

Propriedade

Com a entrega e pagamento dos bens objeto do contrato nos termos do estabelecido na Cláusula 7.^a do presente Caderno de Encargos, ocorre a transferência da posse e da propriedade daqueles para o contraente público, sem prejuízo das obrigações de garantia que impendem sobre o adjudicatário

Cláusula 10.^a

Conformidade e garantia técnica

O fornecedor fica sujeito, com as devidas adaptações e no que se refere aos elementos entregues à Direção Regional de Informática em execução do contrato, às exigências legais, obrigações do fornecedor e prazos respetivos aplicáveis aos contratos de aquisição de bens móveis, nos termos do Código do Contratos Públicos e demais legislação aplicável.

Cláusula 11.^a

Procedimentos ambientais e de gestão de resíduos

1. É da inteira responsabilidade do adjudicatário o destino a dar aos resíduos produzidos ou recolhidos no decurso da sua atividade, sem prejuízo de poder utilizar as estruturas da Entidade Adjudicante destinada à recolha de resíduos, caso exista, e mediante prévia autorização.
2. O adjudicatário deverá desenvolver as atividades objeto do presente procedimento, garantindo o cumprimento das normas ambientais aplicáveis.

Cláusula 12.^a

Responsabilidade

1. O adjudicatário assume a responsabilidade, por si e pelos técnicos seus colaboradores, pela perfeita adequação dos fornecimentos e trabalhos a realizar aos fins a que se destinam.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

2. O adjudicatário é responsável por todos os atos e omissões dos quais possam resultar prejuízos para a entidade adjudicante ou para terceiros, incluindo os praticados através de ação ou omissão dos seus colaboradores, independentemente do vínculo contratual existente, ainda que tais atos ou omissões sejam praticados contra ordens ou instruções que o adjudicatário lhes haja transmitido.

Cláusula 13.^a

Dever de boa execução

Os fornecimentos dos bens e serviços pelo adjudicatário no âmbito do contrato devem cumprir os requisitos exigidos e ser adequados aos objetivos e finalidades definidos pela entidade adjudicante.

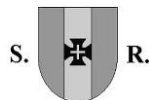
SECÇÃO II – Obrigações da Entidade Adjudicante

Cláusula 14.^a

Preço contratual e formas de pagamento

1. Pela entrega dos bens e fornecimento dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a entidade adjudicante pagará ao adjudicatário o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante, 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 da responsabilidade do fornecedor.
3. O preço a que se refere o n.º 1 será pago de acordo com o seguinte plano:
 - a) 40% com a Entrega, Instalação e Configuração e Aceitação da Componente de Infraestrutura Tecnológica;
 - b) 40% com o Desenvolvimento, Entrega, Instalação e Aceitação da Componente Desenvolvimento Aplicacional;
 - c) 20% com a Formação e Aceitação Global do Projeto, excetuando-se o preço total dos serviços de suporte que serão diluídos no restante prazo de execução do contrato.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Cláusula 15.^a

Condições de pagamento

1. As quantias devidas pela entidade adjudicante nos termos da cláusula anterior, deverão ser pagas no prazo de 60 (sessenta) dias após a receção das respetivas faturas, as quais só poderão ser emitidas após o vencimento da obrigação correspondente.
2. Em caso de discordância por parte da entidade adjudicante quanto aos valores indicados na fatura, deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
3. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas serão pagas através de transferência bancária.
4. O atraso no pagamento das faturas devidas pela Direção Regional de Informática confere ao fornecedor o direito de exigir juros de mora.

Cláusula 16.^a

Deduções nos pagamentos

1. A entidade adjudicante deduzirá nos pagamentos a efetuar ao adjudicatário:
 - a) As importâncias necessárias à liquidação das sanções que lhe tenham sido aplicadas, nos termos do contrato;
 - b) Todas as demais quantias que sejam legalmente exigíveis.

Cláusula 17.^a

Designação de Gestor

1. A entidade adjudicante designará um gestor responsável pelo contrato a celebrar, para efeitos do disposto no artigo 290.º-A do CCP, combinado com o disposto no artigo 8.º-A do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto.
2. O adjudicatário obriga-se, até à data de início do contrato, a comunicar à Direção Regional de Informática, a designação do gestor de contrato responsável pelo contrato celebrado, bem como quaisquer alterações relativamente à sua designação, no prazo de 10 (dez) dias. O gestor deve disponibilizar à respetiva entidade adjudicante, contatos telefónicos, e-mail e de contato direto.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

PARTE IV – PENALIDADES CONTRATUAIS E RESOLUÇÃO

Cláusula 18.^a

Penalidades contratuais

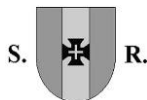
1. Pelo incumprimento de obrigações emergentes do contrato, a entidade adjudicante pode exigir do adjudicatário o pagamento de uma pena pecuniária, calculada de acordo com a fórmula: $P = V \times A / 500$ em que P corresponde ao montante da penalização, V ao valor do contrato e A ao número de dias ou horas de atraso.
2. Na determinação da gravidade do incumprimento, a entidade adjudicante terá em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do adjudicatário e as consequências do incumprimento.
3. O direito à aplicação de penalidades deverá ser exercido pela entidade adjudicante dentro do prazo máximo de 60 (sessenta) dias sobre a data da ocorrência que lhe deu origem.
4. A importância que for devida pelo adjudicatário correspondente às penalidades será deduzida, sem demais formalidades, na fatura a pagamento à data da aplicação da penalidade.
5. As penas pecuniárias previstas na presente cláusula ficam limitadas a 20% ou 30% do valor do contrato, nos termos previstos, respetivamente, nos n.ºs 2 e 3 do artigo 329.º do CCP, consoante o caso que se aplicar.

Cláusula 19.^a

Força maior

1. Não podem ser impostas penalidades ao adjudicatário, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Constituem motivos de força maior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
4. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.





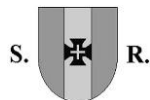
REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Cláusula 20.^a

Resolução do contrato

1. O contrato pode ser resolvido por qualquer das partes em caso de incumprimento definitivo, grave ou reiterado, e culposo por uma das Partes das obrigações por si assumidas no contrato, nos termos gerais de Direito, sem prejuízo das correspondentes indemnizações legais a que houver lugar.
2. Para efeitos do disposto no número anterior, a Parte não culposa comunicará por escrito a ocorrência da situação de incumprimento suscetível de gerar resolução contratual, concedendo à contraparte um prazo não inferior a 30 (trinta) dias para que aquela reponha a situação de incumprimento, sem o que, o incumprimento se tornará definitivo e determinará a resolução contratual, nos demais termos gerais de direito.
3. O contrato pode também ser resolvido pela entidade adjudicante caso se verifique alguma das seguintes situações:
 - a) Quando não se verificar o início dos trabalhos na data acordada pelas partes, por causa direta imputável ao adjudicatário;
 - b) Quando se verificarem atrasos na execução dos trabalhos dos quais resulte impossibilidade da sua conclusão no prazo inicialmente fixado, por causa direta imputável ao adjudicatário;
 - c) Quando os trabalhos tiverem sido subcontratados total ou parcialmente, sem prévia autorização por parte da entidade adjudicante;
 - d) Quando o adjudicatário se recuse injustificadamente a corrigir ou a repetir trabalhos que não forem aceites no âmbito do acompanhamento da execução do contrato;
 - e) Quando o adjudicatário se recuse injustificadamente a cumprir instruções que lhe forem dadas no âmbito do acompanhamento da execução do contrato, para cumprimento do objeto do mesmo;
 - f) Quando se verificar reiterada inobservância das disposições do contrato ou má-fé do adjudicatário;
 - g) Prestação de falsas declarações por parte do adjudicatário;
 - h) Estado de falência ou insolvência;
 - i) Cessaçã da atividade;
 - j) Condenaçã do adjudicatário, por sentença transitada em julgado, por infraçã que afete a sua idoneidade profissional e desde que não tenha ocorrido reabilitaçã judicial.
4. O direito de resolução referido no número anterior exerce-se mediante declaraçã escrita enviada ao adjudicatário.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

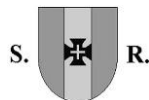
RESOLUÇÃO DE LITÍGIOS

Cláusula 21.^a

Foro competente

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





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

PARTE V – DISPOSIÇÕES FINAIS

Cláusula 22.^a

Comunicações e notificações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato, ou para os respetivos endereços eletrónicos.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 23.^a

Produção de efeitos

O contrato produz efeitos contados da data de aposição de visto por parte da Secção Regional da Madeira do Tribunal de Contas.

Cláusula 24.^a

Contagem dos Prazos

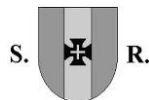
Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados.

Cláusula 25.^a

Legislação aplicável

Em tudo o que não estiver previsto no presente caderno de encargos, aplica-se o previsto no Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, alterado pela Lei n.º 30/2021, de 21/05 e respetiva legislação regulamentar.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

PARTE VI

SECÇÃO I – Especificações Técnicas e Funcionais

Cláusula 26.^a

Arquitetura geral

1. Para a implementação de uma infraestrutura de suporte ao Portal @MADEIRA, pretende-se implementar uma arquitetura composta pelas seguintes componentes:
 - a) Computação;
 - b) Armazenamento;
 - c) Rede Local – LAN;
 - d) Solução de Backups;
 - e) Solução de Ciber-Resiliência;
 - f) Segurança Perímetro;
 - g) Rede Local – Routing;
 - h) Desenvolvimento de software Aplicacional;
 - i) Licenciamento de Software Base;
 - j) Serviços de Desenvolvimento e Implementação;
 - k) Serviços de suporte e acompanhamento;
 - l) Serviços de Formação.

Cláusula 27.^a

Diagrama da Infraestrutura Tecnológica

O concorrente deverá indicar os requisitos técnicos necessários à instalação de todos os componentes da solução, nomeadamente o tipo de circuitos elétricos (monofásicos ou trifásicos) e respetiva amperagem. Deve ainda indicar o espaço físico necessário à correta instalação do equipamento, fornecendo um layout do mesmo. Deverão também ser indicados para efeitos de cálculo da climatização da sala, onde serão instalados os equipamentos, os valores de energia térmica libertada por estes.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

SECÇÃO II – Infraestruturas Tecnológicas

Cláusula 28.^a

Requisitos da Componente de Processamento e Computação

Para dar suporte à componente de computação, pretende-se adquirir uma infraestrutura Hiper convergente.

Entende-se por infraestrutura Hiper convergente, uma solução que agregue num único sistema, capacidade de computação, capacidade de armazenamento, subsistemas de conectividade e software, sendo todas as componentes tratadas como recursos, facilmente alocados consoante as necessidades, criando uma solução de Software Defined Data Center.

O objetivo da entidade adjudicante é eliminar algumas das limitações das infraestruturas tradicionais, de forma a ser possível criar pools de recursos de computação, armazenamento e conectividade, que possam ser consumidas de forma dinâmica, à medida que as aplicações vão necessitando desses recursos, mas de forma unitária e não em bloco, ou seja, permitir a adição de computação, storage ou networking de forma independente.

Entende que numa infraestrutura Hiper convergente, os recursos de computação, storage e networking devem estar abstraídos do hardware onde residem, tornando-os facilmente acessíveis a partir de qualquer ponto do datacenter através de uma interface Web, permitindo o aprovisionamento da exata quantidade de recursos que uma determinada workload necessita, via software.

Pretende-se que a infraestrutura Hiper convergente, permita que os recursos sejam agrupados logicamente, para que a Direção Regional de Informática não precise de configurar fisicamente o hardware que dá suporte a uma aplicação específica, antes definindo os requisitos aplicacionais para a infraestrutura física usando políticas e perfis de serviço para criar a infraestrutura necessária para ser executada em máquinas virtuais.

A infraestrutura Hiper convergente a adquirir pela entidade adjudicante deverá incluir todas as componentes de hardware e software necessárias ao seu funcionamento conforme os requisitos apresentados.

Deverá estar preparada para receber de futuro novas gerações de tecnologia, quer se trate de inovações ao nível da computação, novos medias de storage ou melhorias a nível de largura de banda/latência na conectividade de rede.

O fabricante da solução proposta, deve estar presente no quadrante “Líder” do quadrante mágico da Gartner mais recente, para soluções de infraestrutura Hiper convergente.

A plataforma deve estar certificada na íntegra tanto pelo fabricante do hardware como pelo fabricante do hipervisor.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

A manutenção e as atualizações da solução, devem ser fornecidas de forma unificada, através de um único contrato de apoio, que inclua todo o Hardware e Software fornecido com a plataforma (incluindo SDS e SDC).

A plataforma deve permitir a aplicação de todas as boas práticas recomendadas em relação ao hipervisor, incluindo níveis de resiliência, fatores de proteção, tolerância a falhas e balanceamento de carga em todos os níveis, sem tolerar perda de dados e resposta automática a contingências. O adjudicatário, deve incluir a documentação das boas práticas recomendadas pelo fabricante.

A solução deve ser flexível, para abordar um vasto leque de aplicações e serviços, incluindo a gestão de dados estruturados (como bases de dados) e dados não estruturados (e-mails, documentos e vídeo...) ou desktop virtuais / máquinas virtuais, entre outros exemplos.

Requisitos Técnicos

A solução Hiper convergente, deve disponibilizar, no mínimo 6 nós, com a seguinte configuração mínima, cada:

- a) 2 Processadores Intel Xeon Gold 5218 2.3GHz, 16C/32T ou equivalente
- b) 384GB RAM RDIMM, 3200MT/s, Dual Rank
- c) 2x Discos de 800GB MU SAS SSD para Cache
- d) 10x Discos de 4TB 7.2K RPM 12Gbps para capacidade
- e) 4x portas 10/25 GbE Optical SFP28

Não obstante os pontos acima referidos, a solução deverá disponibilizar no mínimo, 50 TB úteis de armazenamento (excluindo qualquer mecanismo de eficiência), considerando proteção FTT=1. Deverão ainda ser propostos discos que disponibilizem, no mínimo, 1.6TB de cache raw, com pelo menos 2 discos. Não serão aceites soluções com capacidades inferiores às solicitadas. Caso o fabricante da solução recomende um nível de tolerância à falha mais elevado para ambientes de produção, deverá ser considerado esse nível para o cálculo da capacidade útil.

Caso a solução necessite de VM's que consumam recursos da solução para o seu correto funcionamento, as mesmas devem estar claramente indicadas, bem como todos os recursos necessários ao funcionamento das mesmas (memória, CPU, armazenamento). Estes requisitos deverão ser ainda adicionados à solução proposta, não contando como capacidade útil.

A solução deve compreender ainda o fornecimento dos Switches ToR necessários para interligar a solução de Hiper convergência ao Core de rede da Direção Regional de Informática. Estes Switches deverão possuir um mínimo de 16 portas 25GbE Optical SFP28, com portas adicionais de Uplink ao Core de rede 10GbE e respetiva cablagem.

O sistema de armazenamento, deverá ser gerido através de políticas (em vez de grupos de RAID/LUNs/sistemas de ficheiros), que permitam alocar diretamente o nível de desempenho, a qualidade





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

do serviço e proteção de dados necessários, com a granularidade ao nível da VM (objeto). Além disso, o controlo dos níveis de qualidade de serviço (QoS), devem ser fornecidos por VM (Objetos) e deverão poder ser dinamicamente alterados.

A solução deve suportar padrões PCI, para maximizar a segurança da informação e minimizar o risco em caso de queda, perda de dados/corrupção, acesso não autorizado ou falta de conformidade com os níveis e as garantias de serviço.

Deve ser capaz de se proteger contra a falha simultânea de pelo menos 1 elemento do mesmo tipo, sem perda de dados ou serviço (controlador, discos e/ou nó).

Deverá permitir alterar o nível de proteção das máquinas virtuais, a qualquer altura e sem qualquer tipo de quebra de serviço.

Em caso de avaria dos componentes Hardware que constituem o armazenamento, o sistema deverá ser capaz de reconstruir rapidamente os dados na infraestrutura sobrevivente.

A solução proposta deverá permitir a interligação dos nós, com switches de qualquer fabricante, caso assim a Direção Regional de Informática o deseje no futuro.

Características físicas e crescimento

O espaço necessário no datacenter, o seu consumo de energia, as necessidades de refrigeração e outros requisitos e/ou características relevantes em relação à instalação física e operação da plataforma, devem ser indicados de forma precisa e clara. A solução deve implementar estratégias e tecnologias que melhorem a eficiência energética da plataforma.

Nenhuma solução será aceite no limite da capacidade suportada. Para verificar este ponto, deve-se indicar a configuração proposta em relação à capacidade máxima dos nós e do sistema como um todo.

A inclusão na proposta, de funcionalidades em roadmap, ou que não estão disponíveis em versões oficiais (disponibilidade global), não será aceite.

A solução deverá poder crescer de forma horizontal Scale-out, podendo crescer de forma transparente, através da agregação de nós e de forma vertical Scale-up, através da possibilidade de expansão de cada nó (memória, discos e/ou placas de rede). No caso dos discos, deverá permitir o crescimento granular unitário (upgrade de 1 disco em qualquer nó).

Deve ser possível combinar, no mesmo cluster, servidores/nós diferentes e de diferentes capacidades (CPU, RAM, armazenamento) e recursos adicionais (por ex. inclusão de nós com GPUs, NVMe) para permitir um projeto ajustado às necessidades do ambiente e a adaptação a novas cargas de trabalho.

A solução deve ser capaz de escalar para nuvens públicas, permitindo a criação de níveis hierárquicos de armazenamento, usando serviços de armazenamento externos na nuvem como Amazon, Google, Microsoft Azure, OpenStack ou outros.

Todos os componentes da solução devem ser novos. Sistemas com componentes reparados ou recondicionados não serão aceites.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Administração

Todas as operações de interação com o ambiente virtual (computação, armazenamento e rede), deverão ser realizadas através das ferramentas nativas do hipervisor.

Deverão estar incluídas todas as licenças necessárias para todas as funcionalidades solicitadas no presente CE.

A solução não deve limitar ou condicionar as funcionalidades do hipervisor, como:

- a) O uso de snapshots de hipervisor (VM Snaps), que deve continuar a ser gerido de forma transparente para a tecnologia proposta, nativamente e sem perda ou degradação de desempenho, através do software de gestão centralizada.
- b) A capacidade de executar clones, migrações e alocação de recursos no ambiente virtual "quente", sem a necessidade de usar Software de terceiros.

Gestão

A solução deve ser fornecida no modo de assistente de configuração, com o Software necessário já pré-instalado, com o objetivo de minimizar os tempos de implementação.

Deve ser capaz de integrar com as plataformas de monitorização SNMP.

Deverá ser incluída uma plataforma para a gestão e monitorização de hardware e o ambiente de virtualização. A solução deve fornecer uma experiência de suporte integrada, que forneça uma visão dos eventos Hardware e Software, com relatório do status da plataforma e os possíveis incidentes sobre eles, para os administradores e para o fabricante automaticamente (call home). Este mecanismo de suporte remoto, deve certificar adequadamente a sua segurança e a possibilidade de controlar os acessos remotos do suporte do fabricante pelo cliente.

A solução deve realizar análise de falhas de forma preditiva, com notificações proativas de alerta, por meio de mecanismos de deteção automática e alerta comportamental anormal em todo o ambiente (incluindo hardware [CPU, RAM, discos, placas de rede e Interconexão], VMS e mecanismos de proteção)

A escalabilidade da solução proposta, deve ser gerida pela plataforma de gestão. O crescimento do ambiente não tem de gerar mais complexidade na gestão, tendo de automatizar o trabalho de, pelo menos:

- a) Instalação do sistema;
- b) Atualização da plataforma (Hardware e Software);
- c) Expansão de capacidade no(s) nó(s);
- d) Expansão do sistema (adição de nó(s));
- e) Remoção de nó(s);
- f) Substituição de Hardware com falhas;
- g) Shutdown do sistema.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

A plataforma de administração deve incluir recursos de monitorização complementar aos oferecidos pelo hipervisor, que fornecem as métricas necessárias para controlar o estado do ambiente de virtualização e os subsistemas Hardware de uma forma unificada e correlacionada, nomeadamente:

- a) Gráficos de consumo CPU, RAM, IOPS, largura de banda, latência de acesso a dados em todo o ambiente;
- b) Gráficos de consumo CPU, RAM, IOPS, largura de banda, latência de acesso a dados de nós;
- c) Gráficos de consumo CPU, RAM, IOPS, largura de banda, latência de acesso a dados de cada máquina virtual no ambiente.

Deverá ser disponibilizado um portal online pelo fabricante da solução de Hiper convergência que permita de forma centralizada:

- a) Disponibilizar dados de forecast de capacidade e self-optimization recorrendo a mecanismos de Machine Learning.
- b) Permitir visualizar as versões de software instaladas na solução de Hiper convergência.
- c) Permitir visualizar os upgrades possíveis para a solução de Hiper convergência.
- d) Permitir iniciar/agendar o upgrade do(s) cluster(s) de Hiper convergência fornecido(s).
- e) Permitir visualizar o estado de conectividade e saúde da solução de Hiper convergência.
- f) Permitir visualizar o número de máquinas virtuais atualmente a correr no cluster (Power ON, Power off e Suspended).
- g) Permitir visualizar o detalhe a nível de capacidade, Mhz e memória consumidos por cada máquina virtual a correr no(s) cluster(s) hiperconvergente(s)
- h) Permitir visualizar dados de performance do cluster.
- i) Permitir visualizar e detetar anomalias a nível de conectividade, disco, CPU e memória.

A solução deverá ser gerida totalmente (incluindo atualizações/manutenções) num só ponto (vCenter), sem ser necessário recorrer a qualquer outra interface ou consola de gestão.

Atualização/manutenção

A plataforma como um todo, deve ser considerada um único produto, quando se trata de atualizar versões de Software, Firmware e aplicações intrínsecas (por exemplo, plataforma de gestão). O processo de atualização irá fornecer os seguintes recursos:

- a) Deverá ser disponibilizada uma matriz de compatibilidade que reflete a configuração desejável da plataforma, pública e verificada pelo fabricante.
- b) As configurações de destino para cada processo de atualização, deverão detalhar a versão desejável de todos os componentes envolvidos no processo.
- c) O processo deverá ser simples e ágil, sem impacto sobre o ambiente de produção, e executando de uma forma completamente automatizada, uma vez que o administrador da solução, decida iniciar a atualização.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- d) Após a inicialização do processo, a solução deverá ter a capacidade de movimentar automaticamente as máquinas virtuais entre os nós e sem paragem ou intervenção humana, evitando assim qualquer tipo de perda de serviço.
- e) A atualização deverá poder ser realizada, sem a necessidade de intervenção do fabricante da plataforma.
- f) O processo de atualização (Firmware, Drivers, SDS e SDC), deverá ser efetuado diretamente a partir da consola central do hipervisor, de um único ponto/interface e sem necessidade de instalação de software adicional.

Outros Requisitos Técnicos

1. Possibilidade de Scale Up e Scale Out da solução;
2. A solução deverá estar assente numa plataforma que ofereça recursos de computação e storage partilhados, baseado em Software-Defined Storage, Software-Defined Compute, Commodity hardware e ter uma interface de gestão unificada (HCI);
3. A solução deve ter uma única interface de administração das camadas de SDS e hipervisor tendo integração direta, completa e nativa com a consola central do hipervisor, disponibilizando: Dashboard, Vista física e lógica, Gestão do cluster (add/remove), Life cycle management, eService, Marketplace, Gestão de rede.
4. Permitir o crescimento interno dos nós propostos (memória, discos, portas de comunicação, etc.);
5. Possibilidade de crescimento em nós, com diferentes modelos de nós e com configurações flexíveis e não fechadas em termos de possibilidades de armazenamento;
6. Permitir a separação em rede privada do tráfego de gestão do cluster, que permita gestão privada e/ou pública do mesmo;
7. A configuração de memória RAM proposta, deverá cumprir as melhores práticas para preenchimento e ocupação de canais de memória do fabricante do CPU proposto;
8. Deverá permitir adicionar, no mínimo, 2 GPUs aos nós propostos (ou num novo nó, desde que pertencente ao mesmo cluster);
9. Suportar o padrão internacional TPM 1.2 e TPM 2.0;
10. Permitir replicar localmente de forma síncrona (RPO = 0) e assíncrona;
11. Permitir replicar remotamente de forma síncrona (RPO = 0) e assíncrona;
12. Permitir fazer “tiering” e caching de Clouds Públicas e Privadas, com mecanismos de encriptação “in-flight”;
13. Permitir apresentar volumes de storage externos (iSCSI e FC);
14. Possuir mecanismos de caching de Leituras e Escritas, recorrendo a discos solid state;
15. Permitir aplicar QoS ao nível da VM;
16. Permitir aplicar políticas de storage (performance e resiliência) a nível da VM;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

17. Permitir alterar/adequar estas políticas de storage a nível da VM ao longo do ciclo de vida da solução;
18. Tolerância mínima de falha de uma VM = 1;
19. Disponibilizar a funcionalidade FT (fault tolerance), ao nível da VM;
20. Permitir a encriptação de dados ao nível da VM, independentemente do tipo de disco utilizado;
21. Permitir a encriptação de dados ao nível do cluster, independentemente do tipo de disco utilizado;
22. Permitir a gestão intuitiva de Logs, através de dashboards e de forma integrada com o software de virtualização apresentado;
23. Incluir mecanismos de Deduplicação e Compressão;
24. Disponibilizar management packs para integração dos dashboard de logs para o SDS;
25. O software de gestão de Logs deverá ainda suportar role-based access control e integração com a Active Directory;
26. Integração da camada SDS no kernel hypervisor;
27. Incluir driver CSI (Container Storage Interface);
28. Incluir CNS (Cloud Native Storage) Control Plane;
29. Possibilidade de crescer até, pelo menos, 64 nós Hiper convergentes (Computação, Memória e Armazenamento) num único cluster real (não federado);
30. Solução HCI onde a camada SDS não necessite de um storage/controller VM em cada nó para a administração de armazenamento da solução;
31. Um único ponto de contato para o suporte com o fabricante da solução HCI (com vSphere ou equivalente);
32. Possibilidade de configurar as políticas de armazenamento ao nível da VM;
33. Atualização automatizada de toda a solução HCI (hypervisor, SDS, firmware de hardware);
34. Replicação síncrona ao nível da VM;
35. A solução deve disponibilizar os seguintes componentes, integrados de forma nativa:
 - a) Vmware vSAN ou equivalente;
 - b) Vmware vCenter ou equivalente;
 - c) VRealize Log Insight ou equivalente.
36. Incluir todo o licenciamento necessário para o correto funcionamento da solução, bem como cumprimento de todos os requisitos acima referidos;
37. O suporte para hardware e software deverá ser dado diretamente pelo fabricante, on-site, por um período mínimo de 36 (trinta e seis) meses, garantindo tempos de resposta máximos de 4H para todos os componentes propostos (Hardware e Software);
38. Deverá ser fornecido um único número de suporte do fabricante para todos os componentes de Hardware e Software incluídos na solução apresentada;
39. O Hardware proposto deverá ter sido validado e certificado pelo fabricante do hypervisor, não sendo aceites soluções “faça você mesmo”.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

40. A proposta deverá incluir os dados de performance da solução de Hiper convergência proposta para os seguintes workloads: OLTP 32K, OLTP 16K, OLTP 8K, OLTP 4K, RDBMS, TPC.

Cláusula 29.^a

Requisitos da Componente de Armazenamento

A componente de Armazenamento tem como objetivo armazenar a informação do sistema, bem como a criação de um repositório centralizado Dados. Pretende-se para esta componente, a aquisição de uma solução de armazenamento, do tipo Scale-Out NAS, para os quais apresentamos as especificações detalhadas.

Requisitos da Solução de Armazenamento

Por solução Scale-Out NAS, entende-se uma solução que disponibilize:

- Arquitetura Scale-Out – arquitetura de filesystem distribuído, em cluster, combinado com armazenamento modular;
- Crescimento Modular – crescimento modular que inclua computação e armazenamento num único chassis e que integre de forma simples no cluster Scale-Out;
- Sistemas Operativo – baseado num filesystem distribuído que permita a criação de um filesystem virtual único e namespace global a todo o cluster, devendo o filesystem usufruir de funcionalidade de journalling, ser distribuído e com cache de leitura/escrita coerente a todo o cluster;
- Alta Disponibilidade – não deverá possuir pontos únicos de falha, devendo ser capaz de auto remediar falhas de discos ou nós, bem como lidar com falhas de comunicação entre os elementos do cluster;
- Escalabilidade – O cluster deverá escalar de forma fácil, sendo que a adição de novos nós, deverá permitir a autoconfiguração de capacidade e a sua adição automática ao cluster;
- Proteção de Dados – Deverá possuir mecanismos de proteção de dados de forma a suportar a falha de pelo menos 1 nó e de vários discos em simultâneo, sem perda de dados;
- O fabricante da solução proposta, deve estar presente no quadrante “Líder” do quadrante mágico da Gartner mais recente, para sistemas de ficheiros e objetos distribuídos (gartner magic quadrant for distributed file systems and object storage).

Entre outras funcionalidades, a solução Scale Out NAS a adquirir, deverá:

- Permitir uma gestão centralizada dos dados;
- Permitir a hierarquização da informação e políticas automáticas de ILM;
- Ser fiável;
- Ser robusto;
- Ser escalável;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Ser tolerante a falhas;
- Suportar tecnologia de discos SSD (Flash Drives) na plataforma;
- Suportar nativamente, sem recurso a gateways de Hardware ou Software, acessos de última geração REST, OpenStack(SWIFT) e HDFS;
- Implementar tecnologias de eficiência para redução de espaço em disco;
- Suportar a encriptação de dados;
- Escalabilidade massiva para um crescimento virtualmente ilimitado;
- Simplicidade de uso e gestão independentemente do crescimento do volume dados.

Requisitos genéricos

Com esta solução, a entidade gestora do portal @MADEIRA, pretende implementar uma solução robusta, escalável, que permita implementar uma arquitetura Scale-Out NAS, para o rápido crescimento e a melhor partilha de recursos em termos de infraestrutura, como tal a solução a propor deverá:

- Permitir a criação de um filesystem único, que possa crescer numa escala desde as unidades de GB até vários PB, num único namespace, distribuído e transversal a todos os nós/controladores da solução;
- Ser proposta num formato de Appliance, ou seja, as componentes de hardware e software instaladas num único equipamento, que pode ser constituído por vários nós/controladores, em formato Appliance, da mesma marca/fabricante e com suporte técnico único do fabricante da Appliance;
- Ser proposta num formato de Appliance, que disponibilize todas as funcionalidades nos nós/controladores da solução, ou seja, sem utilização de gateways, agentes ou módulos externos ao equipamento proposto, quer para desempenhar parte, ou a totalidade das funcionalidades enumeradas neste Caderno de Encargos;
- Deverá permitir incluir na mesma solução, nós/controladores de diferentes tipos (All-Flash, Híbridos, Arquivo, etc) e de diferentes gerações, promovendo assim a proteção de investimento e facilitando a evolução futura de cada solução;
- Todas as funcionalidades solicitadas no presente CE, deverão estar disponíveis e funcionar em todos os tipos de nós que componham o Cluster/solução;
- Possuir capacidade de balanceamento de utilizadores pelos diversos nós/controladores através de DNS;
- Balanceamento de sessões cliente entre nós/controladores da solução, permitindo o failover e failback de sessões NFS, com o objetivo de otimizar ao máximo a utilização de todos os nós/controladores da solução;
- Permitir integração/autenticação com Active Directory, LDAP, NIS ou através da configuração de utilizadores/grupos locais à solução;
- Capacidade de integrar múltiplas Active Directory no mesmo cluster/solução;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Possibilidade de utilização de múltiplas fontes de autenticação;
- Disponibilizar a função de Auditing da solução, permitindo analisar quem acede/configura a solução, dando assim resposta a requisitos Regulatórios e de Compliance da entidade gestora do portal @MADEIRA;
- Capacidade de replicação integral e total dos dados, entre as duas soluções, assim como definir qualidade de serviço e portas físicas pelas quais se replicam os dados;
- Deverá ser possível definir políticas de replicação ao nível do ficheiro, diretoria ou filesystem total, devendo ser possível definir níveis de prioridade de replicação.
- O software de replicação deverá detetar a ocorrência de uma falha no cluster de produção e efetuar o failover para o cluster remoto. Os utilizadores continuarão a escrever na réplica, até que o cluster principal seja reparado;
- Capacidade de Reporting e Monitorização do sistema, chargeback, taxas de utilização ao nível das várias diretorias, comparação entre reporting com deltas entre os mesmos, etc.;
- Capacidade de aceleração de escritas/leituras através do uso de metadados, fazendo uso de discos SSD ou memória;
- Capacidade de realizar tiering de dados entre níveis de armazenamento de maior performance (Flash) e níveis de armazenamento de menor performance (SAS e/ou NL-SAS), devendo funcionar para todos os nós/controladores da solução e entre distintos tipos de nós/controladores, baseado em políticas definidas pelo administrador, com possibilidade de alteração do esquema de proteção dos dados durante o processo de tiering;
- Tiering deverá poder ser realizado sobre objetos e sobre ficheiros;
- Capacidade de implementar o estado WORM, para maior compliance com normas como a Sec17a-Rule ou equivalente;
- Capacidade de, aquando de upgrades de nós/controladores, os dados serem balanceados de forma automática para maior utilização de todos os recursos disponíveis;
- Capacidade de definir regras para que sempre que existam upgrades, os nós/controladores, serem configuradas de forma automática toda a componente de rede;
- O sistema deve ter a capacidade interna de migrar dados sem impactar a rede LAN na troca ou upgrade de controladores;
- Capacidade de dar mais ou menos prioridade a processos a correrem no sistema;
- O sistema deve permitir a agregação de portas de rede por nó/controlador;
- Capacidade de upgrades de firmware, nó/controlador a nó/controlador, de forma automática, sem perda do acesso aos dados em ambientes NFS;
- O Upgrade de nós/controladores deverá ser online, de forma simples, com balanceamento de dados automático;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Capacidade de balanceamento de dados entre todos os nós/controladores da solução, para evitar “hot spots” e conferir o máximo desempenho possível. O balanceamento de dados deverá ser interno, sem impactar a rede de produção;
- Capacidade on demand de alocar ou retirar portas físicas às subnets/redes associadas;
- Suporte de VLANs, VLAN Tagging;
- Suporte do protocolo IPv6;
- Capacidade de mapear shares de rede via um único IP podendo com isso chegar a qualquer nó/controlador da solução;
- Integração com ambientes analítica hadoop, ou seja, capacidade de funcionar como *um data node* sendo cada controlador um *name node* da solução;
- Capacidade de ter múltiplas distribuições de hadoop a aceder aos mesmos dados;
- Capacidade de utilização de tecnologia SSD para aceleração de dados e metadados, via Caching em SSD (L3 Caching);
- Suportar a funcionalidade de ICAP, para integração com antivírus;
- Suporte nativo dos seguintes protocolos, sem recurso a gateways de Hardware ou Software, ou instalação de Drivers ou Plugins no cliente:
 - NFS: v2, v3 e v4.0
 - CIFS: SMB 1, SMB 2 e SMB 3.0
 - FTP, HTTP/HTTPS, HDFS, REST API, OpenStack SWIFT, NDMP
- Proteção de dados eficiente e resiliente com tecnologia de snapshots instantâneos, sem impacto na performance do sistema, e com velocidade imediata de reposição de dados a pedido;
- Permitir snapshots/cópias remotas de uma diretoria, em simultâneo;
- Suportar deduplicação de dados (deverá ser possível deduplicar quer Objetos, quer ficheiros);
- Capacidade de criação de Quotas, permitindo a monitorização de utilização da capacidade da solução com Reports e criando limites de utilização da solução a vários níveis: Cluster, diretoria, sub-diretoria e ao nível do utilizador ou grupo de utilizadores;
- Deverá disponibilizar a funcionalidade de Soft Quotas: monitorização e reporting da quantidade de armazenamento consumido, mas não tomar qualquer acção;
- Deverá disponibilizar a funcionalidade de Hard Quotas: restringir a capacidade de armazenamento que um utilizador, grupo ou diretoria pode usar e enviar notificações ao administrador da solução;
- Permitir estender o arquivo dos dados para a cloud, privada ou pública;
- Possibilidade de efetuar o arquivo de dados para sistemas de armazenamento Object Storage de baixo custo, que usem protocolo S3;
- Rede interna redundante de alto débito, com Switches redundantes dedicados, no mínimo 10GBE;
- Deverá permitir a replicação assíncrona ou síncrona para outro sistema do mesmo tipo, devendo estar incluído todo o software ou Hardware necessário para o efeito;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Componentes Hot-Swappable: Discos, Fontes de Alimentação e Ventoinhas.

Requisitos relativos a capacidade e especificações técnicas

Deverá ser proposta uma solução, que deverá apresentar os seguintes requisitos mínimos:

- Disponibilizar um mínimo de 300TB Úteis, sem utilização de mecanismos de eficiência de dados (ex: deduplicação), fazendo uso de discos de capacidade não superior a 4TB, com tolerância à falha de 1 nó/controlador completo ou 2 discos em qualquer posição do cluster;
- Disponibilizar um mínimo de 4 nós/controladores;
- Capacidade de ligação a 25 GbE SFP28 (mínimo de 2 portas por nó/controlador) à rede Core da Direção Regional de Informática e ligação a 40 GbE QSFP+ à rede de gestão interna de Backend;
- Mínimo de 128 GB Cache por nó/controlador (mínimo de 512GB por solução);
- Capacidade mínima em discos SSD por cada nó/controlador de 1.6TB Raw, para L3 Caching (6.4TB no total da solução);
- Performance mínima de 1GB/s;

Cláusula 30.^a

Requisitos da Componente de Rede e Comunicações LAN

1. Pretende-se a aquisição de dois switches multi-rate 100GbE de rede aberta de alta densidade e de alto desempenho, otimizado para redes 100GbE leaf / spine e para ligações a sistemas de armazenamento e servidores em rack 25/50GbE de elevada densidade.
2. Cada switch de rede, deverá ser equipado com um mínimo de 64 portas de 100GbE QSFP28 ou até 128 portas de portas 10/25/40 / 50GbE usando cabos breakout.
3. Acesso fácil para SDN para parte ou todo o ambiente de produção.

Cláusula 31.^a

Requisitos da Componente de Proteção de Dados

Pretende-se a aquisição de uma solução de proteção de dados totalmente integrada ao nível de software, hardware, pesquisa e analítica. O hardware a propor deverá ser fornecido em formato de appliance física e que permita endereçar as seguintes necessidades, cumprindo na íntegra com os requisitos técnicos identificados:

- **Solução de Proteção de Dados:**
 - A solução de proteção de dados a propor deverá permitir à Direção Regional de Informática 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.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- O fabricante da solução proposta, deve estar presente no quadrante “Líder” do quadrante mágico da Gartner mais recente, para soluções de backup e recuperação de dados (gartner magic quadrant for data center backup and recovery solutions).
- **Licenciamento da solução de proteção de dados:**
 - Pretende-se a aquisição de um licenciamento totalmente flexível por forma a permitir um melhor enquadramento na realidade da infraestrutura da Direção Regional de Informática, 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 de qualquer fabricante;
 - O licenciamento deverá permitir acomodar tanto as necessidades de backup, como de replicação, monitorização, analítica e pesquisa de metadados.
- **Características e requisitos técnicos da solução de backup:**
 - Entre outras funcionalidades, a solução de proteção de dados a adquirir deverá garantir:
 - Suporte para tecnologia de deduplicação de dados inline e de bloco variável, para otimização dos rácios de deduplicação;
 - A deduplicação entre sites e servidores, independentemente do tipo de dados;
 - Backups rápidos e eficientes para todo o tipo de dados, independentemente da origem;
 - A possibilidade de proteger dados através da integração nativa com arrays de armazenamento primário e de tecnologia de snapshot para redução de impacto no backup;
 - A possibilidade de replicação eficiente ao nível de rede e suporte para vários métodos de replicação (1:1, n:1, 1:n);
 - A possibilidade de exportar dados diretamente para cloud (pública 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;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- 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 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;
- 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 totalmente integrada em formato de appliance e suportada a partir de um único fabricante.

Descrição da Infraestrutura a Proteger

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

- 1) Capacidade de proteção de dados nos Datacenters do Governo Regional da Madeira para a solução constante no presente Caderno de Encargos, considerando um volume de dados estimado em:
 - 240TB úteis de espaço em ambientes virtualizados;
 - Considerar que serão dados aplicativos e dados documentais.
- 2) Política de backup consistente com:
 - Backup full diário + backup logs;
 - Período de retenção em disco por um período mínimo de 30 dias para recuperações operacionais rápidas, backups mensais e anuais para retenção de longo termo;
 - Consideração de taxa de crescimento anual de 10% para um período de 5 anos.
- 3) Capacidade de performance e escalabilidade necessárias para assegurar proteção de investimento e futuras necessidades:
 - Capacidade de escrita correspondente a até pelo menos 32TB/hora;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Capacidade de expansão, sem recurso a troca de controlador de até pelo menos 240TB úteis, excluindo efeitos de deduplicação e/ou compressão;
 - Suporte para protocolos NFS/CIFS, VTL e OpenStorage (e em simultâneo se necessário);
 - Capacidade de backup direto para o repositório de dados, sem recurso a software de backup, para aplicações Hadoop, Oracle, SAP, SAP HANA e Microsoft SQL.
- 4) 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.
- 5) A solução deverá fornecer e incluir todo o software necessário ao funcionamento da mesma, incluindo a de encriptar os dados *at rest*. A capacidade de encriptação deverá ser possível sem necessidade de recurso a hardware dedicado, como por exemplo, discos específicos para encriptação.
- 6) A solução deverá ser fornecida sem limites de clientes e/ou agentes aplicacionais.
- 7) A replicação deverá ser efetuada no menor espaço de tempo possível, por forma a permitir o backup regular dos logs e salvaguarda dos mesmos por via de replicação;
- 8) No sentido de garantir a mínima integridade dos dados armazenados, a solução deverá contemplar ao nível do repositório de dados os seguintes níveis mínimos de redundância e validação:
- Fontes de alimentação redundantes;
 - Proteção de disco de dupla paridade (RAID6);
 - Mecanismo de verificação de integridade dos dados durante a escrita.
- 9) A componente de hardware deverá ainda ser fornecida em formato PBBA (Purpose-Built Backup Appliance), ou seja, ter um conjunto de características diferenciadoras dos restantes dispositivos appliances e storage arrays tradicionais, onde se destaca:
- Serem capazes de armazenar especificamente dados de backup no formato do software de backup, sendo impraticável o uso dos dados para outros propósitos;
 - Implementação de elevadas taxas de deduplicação (normalmente 10:1 ou mais), sendo impraticável o uso dos dados para outras tarefas que não recuperações;
 - Permitir a replicação de dados em elevada eficiência (maioritariamente devido à deduplicação dos dados) por forma a facilitar backups rápidos a partir de localizações remotas;
 - Fornecer tradução de protocolo (p.e. S3, OpenStack) para transferência de dados para repositórios de cloud (“cloud tiering”).

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





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Integrações e suportabilidades

Deverá ser proposta uma nova solução de proteção de dados, capaz de permitir à Direção Regional de Informática 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 por forma a:
 - a. permitir a gestão e operação diretamente a partir do UI de gestão nativo;
 - b. Integração com blueprints do fabricante, por forma a permitir aprovisionamento de proteção de dados diretamente a partir do catálogo de serviços;
 - c. Suporte para backup através de HotAdd, NBD / Fallback;
 - d. Recuperação Granular ao nível da VM, sem recurso a agente na VM;
 - e. Operação self-service tanto para backup e recuperação de VMs.
2. Suporte para API REST para integração com portais de gestão e aprovisionamento.

Cláusula 32.^a

Requisitos da Componente de Ciber-Resiliência

Dada a criticidade da informação relativa ao projeto @MADEIRA, deverá ser proposta como componente integrante da solução a propor, uma componente de proteção contra ciberataques, que permita à Direção Regional de Informática recuperar com a maior rapidez possível e com a garantia de confiança de recuperabilidade, a informação crítica da gestão documental. A solução proposta deverá incluir todas as componentes de software, hardware (servidores, redes, etc) pesquisa e analítica que permita identificar potenciais ameaças e vetores de ataque, capaz de permitir à Direção Regional de Informática recuperar a informação crítica da gestão documental e em caso de destruição, comprometimento ou encriptação maliciosa da mesma em produção, que contemple os seguintes requisitos mínimos:

1. Capacidade de proteção dos dados da gestão documental, incluído as suas componentes core (aplicação, documentos, etc) e os serviços base associados (DNS, Active Directory, etc).
2. Política de proteção consistente com:
 - a. Proteção de toda a informação crítica da solução de gestão documental;
 - b. Mínimo de retenção em disco, de 15 pontos no tempo;
 - c. Validação automática da integridade da informação para pelo menos 15 pontos no tempo (cópias “Gold”).

A solução deverá procurar garantir a automação e fluxo de trabalho para pelo menos 15 cópias “Gold”, para um segundo repositório o qual tem de replicar nativamente com o repositório de proteção em proteção, para que os processos de negócios possam ser retomados após um ataque destrutivo. Deverá concentrar-se nos seguintes pilares de proteção e recuperação:





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Planeamento e design, por avaliação dos sistemas e aplicações críticas para o negócio, objetivos de recuperação para adequar a implementação da solução. A incluir a criação de mapeamentos de dependências com a infraestrutura associada, metadados, etc.;
- Isolamento (físico e lógico) da rede de produção, com replicação através de link dedicado, controlado exclusivamente a partir da área de isolamento e sem qualquer dependência da produção para a gestão e operação da solução contra ciber-ataques;
- Componente de Analítica, que permita salvaguardar o bom funcionamento e eficácia da solução a propor, por forma a dar a visibilidade necessária para a garantia de recuperabilidade da informação isolada;
- Restauro e recuperação, de acordo com os padrões que a solução disponibiliza, acrescido de considerações especiais a aplicar conforme os cenários apresentados, por plano de resposta a ciber-incidentes, incluir avaliação forense e de dano aos dados, a preparação da recuperação a partir das imagens “Gold” das aplicações e binários de sistemas operativos, a culminar no retorno do ambiente de produção à sua operação normalizada.

Para além disto deverão ser assegurados os seguintes requisitos técnicos:

1. Isolamento seguro da solução através de “air-gap” com conectividade dedicada;
2. Gestão e operação da solução sem qualquer dependência da produção, incluindo a componente de analítica, permitindo uma redução da superfície de ataque;
3. A componente de analítica deverá efetuar análise aos dados salvaguardados, na área de isolamento. A análise deverá incidir sobre todas as estruturas de um ficheiro (metadata de ficheiro, metadata de documento e conteúdo) por forma a aumentar a eficácia de deteção e reduzir falsos positivos;
4. Todos os dados salvaguardados na solução deverão ser em formato imutável e certificável, por forma a impossibilitar um único recurso a poder alterar, modificar, adulterar ou apagar qualquer tipo de informação protegida;
5. Recuperação automática iniciada a partir da solução de isolamento, através de REST API, User Interface ou CLI;

Cláusula 33.^a

Requisitos da Componente de Segurança de Perímetro

O equipamento de segurança de informação visa garantir o cumprimento das Diretivas Comunitárias NIS2. As suas características técnicas ao nível de performance, disponibilidade e solução estão de acordo com os requisitos indicados na Resolução do Conselho de Ministros N.º 41/2018, de 28 de março.

Especificações técnicas da Solução de Firewall





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Hardware (obrigatório dentro do mesmo equipamento):

- Número de portas 10Gbit/s RJ45 ≥ 4
- Número de portas Gigabit SFP+ 10Gbit/s ≥ 16
- Número de portas Gigabit QSFP+ 40/100 Gbit/s ≥ 4
- Discos rígido SSD em RAID para sistema $\geq 2 \times 240\text{GB}$
- Discos rígido SSD em RAID para Log $\geq 2 \times 2\text{Tb}$
- Porta de gestão dedicada "Out of Band"
- Porta de consola RJ45
- Arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção.
- Deverá estar garantido que a appliance de Firewall quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa.
- Fontes de alimentação redundantes.

Performance:

- Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção) $\geq 37,0 \text{ Gbps}$
- Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) $\geq 23,0 \text{ Gbps}$
- Performance da appliance com a funcionalidade de VPN IPSec $\geq 18,0 \text{ Gbps}$
- Número de novas sessões por segundo $\geq 380\,000$
- Número máximo de sessões $\geq 8\,000\,000$

Gestão:

- Gestão e administração da própria appliance através de interface web, linha de comandos e API XML;
- Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio;
- Deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy;
- Possibilidade de editar configurações pendentes que ainda não foram aplicadas;
- Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas;
- Possibilidade de descartar alterações à configuração realizadas;
- Possibilidade de armazenar diferentes versões da configuração;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda a infraestrutura instalada;
- Stacks de templates com configurações reutilizáveis para múltiplos equipamentos;
- Ponto centralizado para efetuar upgrades e atualizações de versões e assinaturas;
- Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão;
- Zero Touch provisioning para simplificar o deployment de firewalls remotas;
- Gestão centralizada de SD-WAN para os escritórios remotos;
- Análise da utilização das regras para reduzir superfície de exposição e melhorar postura de segurança;
- Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento;
- Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça;
- Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade.

Networking:

- As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3;
- Suporte de IEEE 802.1Q;
- Suporte de IEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo;
- Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP;
- Suporte de routing estático;
- Suporte de DHCP, NAT e PAT;
- Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas;
- Capacidade de realizar policy based routing através do IP ou rede de origem;
- Capacidade de realizar policy based routing através do tipo de aplicação;
- Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo;
- Permitir a criação de clusters de alta disponibilidade até 6 membros;
- Suporte para TLS 1.3 e capacidade de descriptar este tráfego.

Identificação de Utilizadores:

- Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory;
- Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores;
- Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores;
- Possibilidade de gerir utilizadores através de API XML;
- Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local;
- Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing.

Funcionalidades Gerais de Segurança:

- Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança;
- Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança;
- Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino;
- Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas;
- Capacidade de identificação de subfunções dentro de uma aplicação;
- Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7;
- Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações;
- Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP;
- Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP;
- Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL;
- Capacidade de decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling);
- Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego;
- Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Capacidade de forçar o uso de MFA para acesso a aplicações internas;
- Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes.

IDS/IPS:

- Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças;
- Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas;
- Possibilidade de escolher proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos;
- As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma que a aplicação de perfis de proteção se possa realizar com base nestas categorias;
- Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades;
- Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis;
- Deve ser possível converter assinaturas snort e suricata para dentro da plataforma.

Antivírus & Anti-Malware:

- Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C;
- Capacidade de habilitar mecanismos de DNS sinkholing que permitam interceptar pedidos de resolução de nomes para domínios comprometidos com malware;
- Capacidade de definir políticas de antivírus, de forma que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso;
- Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs);
- Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possam tomar uma ação no caso de um ficheiro malicioso;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações;
- Capacidade de identificar ficheiros não através das suas extensões, mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros;
- Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente;
- Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro;
- Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança;
- Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados;
- Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing;
- Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças.

URL Filtering:

- Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar (permitir, bloquear, permitir, mas advertir, etc);
- Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud;
- Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação);
- Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web;
- A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas.

DNS Security:

- A solução deve disponibilizar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos;
- Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes;
- A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling);
- A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS;
- Este serviço deve permitir identificar quais as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente;
- A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente;
- Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas;
- Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos;
- Devem ser disponibilizadas as seguintes categorias para construção de políticas: Command and Control Domains, Malware Domains, Dynamic DNS Hosted Domains, Newly Registered Domains, Phishing Domains, Grayware Domains and Parked Domains;
- A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças;
- A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas;

Sandboxing:

- Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload);
- Perante uma análise por parte do serviço de Sandboxing na cloud que categorize a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente);

- O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios;
- A tecnologia de Sandboxing tem que ser capaz de inspecionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP;
- A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução;
- Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux;
- O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida;
- Em termos de suporte de sistemas operativos Windows emulados deve suportar: Windows XP, Windows 7 e Windows 10;
- Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS);
- Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF);
- Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado;
- Capacidade de descriptar malware (unpacker) para utilização na análise estática e machine learning.

IOT Security:

- A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT;
- A firewall deve colecionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede;
- A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camera de vigilância), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo;
- Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também;
- Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal;
- A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas;
- Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos, ETC;
- O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associadas ao uso/configuração incorreta dos mesmos. Exemplo: uso de credenciais default;
- Deve existir a possibilidade do Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB(Cloud Access Security Broker).

Data Loss Prevention:

- A plataforma deve disponibilizar um módulo completo de Data Loss Prevention;
- Esta funcionalidade deve ser disponibilizada como um serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente como por exemplo: Financeiros, Legais, Saúde, informação pessoal, etc. A solução deverá também permitir controlar este tipo de documentos de forma evitar a sua exposição ou extravio;
- Este serviço deverá permitir proteger estes documentos das seguintes formas:
 - Prevenir o upload de ficheiros com informação confidencial e/ou sensível para aplicações web não permitidas pela organização;
 - Monitorizar o upload de documentos para aplicações externas permitidas pela organização.
- O serviço deve disponibilizar out-of-the-box pelo menos 380 “data patterns” e deve também disponibilizar perfis que agrupam determinados padrões de forma a simplificar a criação de políticas.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Por exemplo, deverá existir um perfil associado com o GDPR de forma a facilitar a monitorização de documentos que possam conter informação pessoal de utilizadores;

- Deverão existir os seguintes perfis out-of-the box: Bulk CCN, CCPA, Corporate Financial docs, Financial information, GDPR, GLBA, Healthcare, Intellectual Property, Legal, Malware, Personally-Identifiable Information, Profanity, Self Harm e Sensitive content;
- A solução deverá ser constantemente atualizada com novos padrões e perfis;
- De forma a melhorar o rácio de deteção e eliminar falsos positivos a solução deverá permitir especificar: proximity keywords, níveis de confiança e expressões regulares básicas ou “weighted”;
- Este serviço deve poder ser consumido por diferentes plataformas do fabricante, nomeadamente, firewalls, serviço SASE(Secure Access Service Edge), CASB(Cloud Access Security Broker) e CSPM(Cloud Security Posture Management). Isto permitirá aplicar políticas de DLP transversais à organização.

SD-WAN:

- Deve ser possível através de licenciamento adicional adicionar um módulo de SD-WAN à plataforma;
- A plataforma deve permitir adicionar um overlay de SD-WAN que permita escolher de forma inteligente e dinâmica os links mais apropriados para envio de tráfego;
- Deve ser possível criar regras de SD-WAN por aplicação e definir os requisitos mínimos para cada link. No caso de os requisitos mínimos não serem cumpridos pelo link em uso, deve ser feito o failover do tráfego automaticamente;
- Para os links deve ser possível monitorizar e definir regras com base em: latência, jitter e perda de pacotes;
- A plataforma deve permitir fazer load-sharing através de múltiplos links de forma a melhorar o aproveitamento da largura de banda disponível;
- As firewalls devem suportar a funcionalidade de zero-touch provisioning;
- A plataforma deve disponibilizar informação sobre a performance das aplicações e links;
- Esta funcionalidade deve ser gerida centralmente através de uma única consola;
- Deve ser suportada a funcionalidade de Packet duplication, o que permite a um equipamento enviar o mesmo pacote em links diferentes. O equipamento que recebe ambos os pacotes deverá descartar o último a chegar;
- Deve ser suportada a funcionalidade de Forward Error Correction.

Relatórios & Logs:

- A appliance deve ter a capacidade gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas;
- Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf;
- Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets;
- Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende;
- Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento;
- Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a longo prazo;
- Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema;
- Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviado ao serviço de sandboxing e equipamentos internos comprometidos;
- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma que a partir dos logs criados se possa obter informações de alto nível.

Outras Funcionalidades:

- Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade;
- Possibilidade de decifrar tráfego SSL e SSH de forma que se possa estabelecer políticas de descriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados;
- Capacidade de criar exceções à descriptação para determinado tipo de tráfego;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC);
- Possibilidade de enviar tráfego após descriptação para uma interface de port mirror para análise de terceiras partes;
- Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego;
- Capacidade de capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção.

Mapa de Quantidades:

Descrição	Quantidade
Appliance de Segurança em alta disponibilidade (HA) com 25 contextos Virtuais	1(1 clusters)
Duas Appliances Físicas de Gestão para aguentar com o Logging e gestão de toda infraestrutura	1 Equipamento
Licenciamento, com subscrição de suporte funcionalidades por 36 meses: • Firewall Aplicacional (Layer7) • Controlo de utilizadores • DLP – Controlo de conteúdos dos ficheiros • Threat Prevention; • IDS/IPS • Antivírus & Anti-Malware • URL Filtering • Sandboxing • Analise de eventos • Reporting	1 Cluster





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Secção III – Desenvolvimento Aplicacional da Plataforma @MADEIRA

Cláusula 34.^a

Requisitos da Componente de Desenvolvimento Aplicacional

1. Enquadramento

A Plataforma @MADEIRA visa fornecer aos utilizadores uma forma simples e atrativa de aceder a um vasto conjunto de informações e ofertas através de aplicações móveis. Este portal permitirá interligar os organismos do Governo Regional da Madeira aos operadores económicos da Região e aos milhares de turistas que visitam anualmente a Madeira e o Porto Santo, estando definidos dois objetivos primordiais:

- a) Tornar a experiência do turista única e inesquecível;
- b) Promover a oferta económica e turística da Região.

A Plataforma Aplicacional deverá incluir dois módulos interligados, designadamente:

- a) Módulo de Apoio à Atividade Comercial;
- b) Módulo de Visitas Virtuais à Região.

Esta plataforma deverá, recorrendo a tecnologias de Inteligência Artificial, criar um perfil do utilizador e direcioná-lo para os roteiros mais adequados aos seus gostos e prioridades. O acesso à plataforma por parte do turista será feito através de uma plataforma mobile.

Por outro lado, esta plataforma deverá disponibilizar um conjunto de serviços adicionais direcionados à entidade gestora do portal @MADEIRA e aos Operadores Económicos, designadamente:

- a) Um portal de Parceiros onde os Operadores Económicos publicarão as suas ofertas e serviços;
- b) Um Portal de Customização onde a entidade gestora do portal @MADEIRA validará, certificará e adequará as ofertas aos vários perfis de turistas;
- c) Plataforma de Data Management e Intelligence que apresente informação crucial sobre os turistas, como e por onde se deslocam durante a sua estada, e como se relacionam com a economia da região;
- d) Plataforma de Análise que permita observar se os indicadores de performance definidos estão a ser cumpridos;
- e) Motor de Inteligência Artificial que, de forma dinâmica e com mecanismos de autoaprendizagem, construa um perfil do turista de acordo com a sua atividade e com base nos inputs;
- f) Sistema de Análise Preditiva que permita aos operadores económicos e à entidade gestora do portal @MADEIRA assignar as ofertas adequadas ao perfil de turista;
- g) Sistema de Visitas Virtuais à Região.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

2. Requisitos da Plataforma Aplicacional @MADEIRA – Módulo Apoio à Atividade Comercial

A plataforma @MADEIRA deverá incluir um conjunto de módulos interligados de forma a cumprir os requisitos. Nesta secção enumeramos os requisitos de cada um dos módulos.

2.1. Plataforma Mobile para o Turista

A Aplicação Mobile funcionará como um Guia Personalizado para o Turista. Esta aplicação deverá cumprir os seguintes requisitos:

Compatibilidade e funcionalidades base:

- Ser Compatível com Plataformas IOS e Android, sendo da responsabilidade do proponente a publicação nas respetivas lojas (App Store e Play Store);
- A Plataforma Mobile deverá solicitar autorização para partilha de localização através do sistema do Smartphone.

Processo de Registo:

- Processo de registo que inclua os dados do Turista, incluindo endereço email, Agregado Familiar, Faixas Etárias, Duração da Estadia, Local de Alojamento, Proveniência, bem como outras informações definidas em sede de projeto;
- O Processo de registo deverá incluir também uma matriz de preferências para o Agregado Familiar de forma a criar o perfil de turista;
- O processo de registo deve estar conforme as normas do Regulamento Geral de Proteção de Dados; nesse sentido, qualquer recolha de dados deverá incluir o processo de aceitação por parte do utilizador.

Bonificações:

- Após registo, o Turista receberá um conjunto de cupões de desconto, sendo que cada cupão tem um QR Code associado;
- Os cupões de desconto serão atribuídos em virtude do perfil do Turista;
- Os cupões poderão ser descontados juntos dos parceiros aderentes, apresentando um QR Code no momento da transação.

Roteiros e Sugestões:

- Após o registo será apresentado ao Turista um roteiro de acordo com o seu perfil. Esse registo será apresentado em formato de Lista ou Mapa;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Com base nesse registo será feito um calendário de atividades de acordo com o perfil do turista, suas preferências e duração da estadia;
- Os locais (sejam estabelecimento ou pontos de interesse) sugeridos, apresentados em lista ou mapa, mostrarão, quando selecionados, detalhes sobre o local.

Registo de Atividades:

- A aplicação deverá recolher em tempo real, através de geo-referenciação, os percursos do turista;
- Adicionalmente, o utilizador pode registar em Fotografia ou Vídeo as suas atividades e adicionar ao registo do local. (Se, por exemplo, o turista optar por uma das múltiplas levadas da Madeira, tem a possibilidade de - através da App - gravar todo o percurso da levada e anexar fotografias e vídeo, ambos georreferenciados, para visualizar à posteriori);
- O utilizador deverá também poder registar a visita a um local através da leitura de um QR Code localizado no Ponto de Interesse.

Gamificação:

- Para incentivar o uso da Plataforma, e com isso maximizar a sua utilização e dos dados por ela fornecidos, a mesma tem uma vertente de Gamificação que atribui pontos quando o turista se desloca a determinados locais;
- Os pontos poderão ser convertidos em cupões de desconto adicionais a selecionar pelo utilizador na lista que lhe será disponibilizada.

2.2. Plataforma para o Parceiro Económico

Deverão ser disponibilizadas duas plataformas para o Parceiro Económico:

- Uma aplicação assente numa plataforma mobile para registo de utilização dos cupões de desconto;
- Uma aplicação de Gestão onde o Parceiro Económico regista e atualiza as suas ofertas de serviços.

Apresentamos de seguida os requisitos funcionais para cada uma das plataformas.

Aplicação Mobile para o Operador Económico:

- Esta aplicação deverá ser compatível com Plataformas Apple IOS™ e Google Android™, sendo da responsabilidade do proponente a publicação nas respetivas lojas (App Store e Google Play);
- A Plataforma Mobile deverá solicitar autorização para partilha de localização através do sistema do Smartphone;
- A Plataforma Mobile para o Turista tem armazenados Cupões de Desconto que podem ser utilizados nos Parceiros Aderentes para aquisição de bens e serviços;
- Os cupões de desconto estão referenciados com um QR Code que identifica o utilizador Turista e qual o benefício assignado ao cupão;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- A Plataforma Mobile deverá ter a capacidade de ler o QR Code do cupão de desconto, registar a atividade do utilizador e abater o cupão após utilização;
- Da mesma forma, e de forma a garantir a fidelização do utilizador turista, a Plataforma Mobile para o Operador Económico poderá, se assim o desejar, atribuir um novo cupão de desconto ao utilizador;
- A Aplicação de Registo deverá ter mecanismos de autenticação que validarão o acesso do Operador Económico.

Aplicação de Gestão para o Operador Económico

- A aplicação de Gestão para o Operador Económico é o veículo através do qual o Operador pode lançar promoções, publicar cupões de desconto, publicitar as suas ofertas e fazer a gestão da sua oferta;
- Esta deverá ser uma plataforma Web Based através da qual o Operador pode aceder através de um Browser;
- Esta aplicação deverá estar otimizada de forma a ser acedida através de múltiplas plataformas, nomeadamente Computador, Tablet ou Smartphone;
- A aplicação deverá ter mecanismos de autenticação seguros;
- A aplicação deverá ter um sistema de registo de utilizador para identificação do Operador Económico;
- A aplicação deverá ter mecanismos para criação de novos utilizadores no Operador Económico, com definição de permissões dentro da Aplicação de Gestão e da Aplicação Mobile.

2.3. Portal de Customização

O Portal de Customização é a plataforma através da qual a entidade gestora do portal @MADEIRA faz a gestão das ofertas dos parceiros económicos e as cruza com os perfis de utilizadores turistas:

- Esta deverá ser uma plataforma Web Based através da qual o Operador pode aceder através de um Browser;
- Esta aplicação deverá estar otimizada de forma a ser acedida através de múltiplas plataformas, nomeadamente Computador, Tablet ou Smartphone;
- A aplicação deverá ter mecanismos de autenticação seguros;
- A aplicação deverá ter um sistema de registo de utilizador para identificação do utilizador;
- A aplicação deverá ter mecanismos para criação de novos utilizadores no Portal de Customização, com definição de permissões;
- A plataforma deverá identificar os perfis de Turistas criados pelo Motor de Inteligência Artificial e apresentar sugestões das melhores ofertas promocionais;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- A plataforma deverá permitir monitorizar e gerir em tempo real a utilização dos cupões e atividades dos turistas.

2.4. Plataforma de Data Management e Intelligence

- A plataforma de Data Management e Intelligence é uma componente do Portal de Customização;
- Deverá permitir elaborar relatórios detalhados e customizados de registo de atividades para a equipa de gestão da entidade gestora do portal @MADEIRA;
- Deverá permitir elaborar relatórios personalizados para cada operador económico;
- Deverá permitir a definição de KPIs para monitorização do sucesso das atividades e promoções;
- Deverá estar integrada num módulo independente dentro do Portal de Customização.

2.5. Motor de Inteligência Artificial

Esta componente terá como objetivo:

- Criar de forma dinâmica Perfis de Turistas;
- Analisar em tempo real a atividade dos turistas, a sua adesão às promoções e os roteiros e percursos por estes realizados;
- Analisar em tempo real as ofertas disponíveis lançadas pelos operadores económicos e assigná-las aos perfis de turistas;
- Efetuar uma análise de sucesso das novas ofertas lançadas pelos operadores;
- Apresentar recomendações aos operadores económicos para lançamento de campanhas e ofertas de sucesso, com a capacidade de criar ofertas tipo bundle (ou seja, que juntem vários operadores numa oferta única);
- A solução deverá utilizar tecnologias de Machine Learning de forma a conseguir criar dinamicamente novos padrões.

2.6. Plataforma de Integração

- A plataforma de integração assegura a correta comunicação entre todas as componentes da aplicação, designadamente Plataforma Mobile para o Turista, Plataforma para o Operador Económico, Portal de Customização, Plataforma de Data Management e Intelligence e Motor de Inteligência Artificial;
- A plataforma deverá utilizar protocolos seguros e comunicações encriptadas entre todas as componentes;
- Deverá integrar a funcionalidade de controlo de versões e upgrades, assegurando a correta e continua integração entre todas as componentes.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

3. Requisitos da Plataforma Aplicacional @MADEIRA – Módulo de Visitas Virtuais

3.1. Enquadramento

Esta Plataforma pretende implementar um portal de apresentação de pontos turísticos para visitas virtuais. Esta componente deverá cumprir com as seguintes Funcionalidades Gerais:

1. Mapa com pontos turísticos categorizados e georreferenciados onde será possível visualizar ou ouvir os conteúdos a ele ligados:
 - a) Será possível adicionar vídeos, fotografias 360 graus, fotos para slide show, ficheiros de som com relatos ou explicações.
2. Quando um turista visita os pontos, cada conteúdo visto ou ouvido fica registado como visitado e, se visualizar ou ouvir uma determinada percentagem dos conteúdos aquele ponto fica marcado
 - a) Pontos visitados podem ser comentados e avaliados para além de poderem marcar como “desejo visitar fisicamente”;
 - b) Os comentários serão mediados por um moderador;
 - c) Serão atribuídos rankings a quem visitar um determinado número de pontos e os seus comentários e avaliações apresentarão esse ranking;
 - d) O visitante poderá reportar um comentário.
3. Será possível entidades ou privados carregarem novos pontos que, depois de aprovados, passam a fazer parte da oferta:
 - a) A aprovação destes pontos poderá ser feita administrativamente pela entidade gestora do projeto @MADEIRA ou por votação pelos agentes económicos por forma a aumentar a interatividade entre a oferta turística e a população em geral;
 - b) Na proposta devem ser submetidos conteúdos, descrições e justificação. Que depois serão geridos pela entidade gestora do projeto @MADEIRA;
 - c) Será também atribuído um ranking a quem mais propõe pontos aprovados e também sobre o número de visitas e avaliações desses pontos que lhes ficam associados.
4. Os pontos estarão ligados pelas categorias para permitir sugestões de outros pontos ao visitante caso não esteja autenticado. Tendo em conta os pontos já visitados e o perfil do visitante também se poderá fazer propostas diretamente ao visitante:
 - a) Apresentar outros pontos que possam interessar ao visitante logo na página de cada ponto;
 - b) Envio de email com propostas de pontos a visitar se o visitante não for à plataforma durante um tempo com Pontos que podem interessar, Novos pontos e Relatório de conquistas.
5. Um visitante deverá poder fazer uma tour onde lhe serão apresentados os conteúdos de vários pontos em sequência:
 - a) Os conteúdos a apresentar deverão poder ser selecionados ou escolhidos de forma aleatória na altura da apresentação;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- b) Deverão estar disponíveis tours pré-definidas pela entidade gestora do projeto @MADEIRA, que o visitante poderá escolher para visualizar de vários pontos relacionados pela categoria ou tipo;
- c) Os visitantes poderão criar e guardar as suas próprias tours que poderão visualizar várias vezes ou partilhar com outros utilizadores.

3.2. Plataforma de controlo

Nesta plataforma será possível à entidade gestora do projeto @MADEIRA fazer a manutenção de toda a informação disponível no portal, desde os conteúdos até à mediação dos comentários:

- 1. Esta deverá ser Web Based onde o Operador poderá aceder através de um Browser;
- 2. Esta aplicação estará otimizada de forma a ser acedida através de múltiplas plataformas, nomeadamente Computador, Tablet ou Smartphone;
- 3. A aplicação deverá ter mecanismos de autenticação seguros;
- 4. A aplicação deverá ter um sistema de registo de utilizador para sua identificação;
- 5. A aplicação deverá ter mecanismos para criação de novos utilizadores no Portal de administração, com definição de permissões;
- 6. Deverá ser possível adicionar vídeos, fotografias 360, fotos para slide show, ficheiros de som com relatos ou explicações por cada ponto de interesse para além dos dados gerais desse ponto, nomeadamente o nome e georreferenciação;
- 7. A plataforma deverá permitir monitorizar e gerir em tempo real a utilização do portal público, com número de visitantes online, visitas, comentários e propostas.

3.3. Portal Público

No portal público será possível navegar num mapa com pontos georreferenciados cada um deles com conteúdos em texto, imagem, vídeo ou áudio que permitirão realizar uma visita virtual ao local.

1) Compatibilidade e funcionalidades base:

- a) Este portal deverá ser Web Based onde o visitante poderá aceder através de um Browser;
- b) Este portal estará otimizado de forma a ser acedido através de múltiplas plataformas, nomeadamente Computador, Tablet ou Smartphone;
- c) A aplicação poderá ser utilizada por visitantes registados e anónimos, sendo que algumas funcionalidades não estarão disponíveis para os visitantes anónimos;
- d) A aplicação deverá ter um sistema de registo de utilizador para identificação dos utilizadores que pretendam utilizar todas as funcionalidades da plataforma;
- e) A aplicação deverá ter mecanismos de autenticação seguros para os visitantes registados.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

2) Processo de registo:

- a) O processo de registo deverá incluir os dados do visitante como o nome, email e categorias preferidas, bem como outras informações definidas em sede de projeto;
- b) O processo de registo deverá estar conforme as normas do Regulamento Geral de Proteção de Dados; nesse sentido, qualquer recolha de dados deverá incluir o processo de aceitação por parte do utilizador.

3) Utilização do portal:

- a) O mapa usará como base o sistema google® maps® ou semelhante e permitirá utilizar as funcionalidades básicas desse sistema, zoom, navegação, múltiplas vistas, etc;
- b) Os pontos serão apresentados com uma pop-up com a categoria, pontuação, e uma imagem de pré-visualização;
- c) Cada ponto, quando selecionado, abrirá uma nova página com a totalidade dos conteúdos a ele associados, a lista de comentários, pontuação e uma sugestão de outros pontos da mesma categoria;
- d) Deverá ser possível usufruir de todos os conteúdos diretamente da plataforma sem necessidade de software externo;
- e) Quando um turista visita os pontos, cada conteúdo visto ou ouvido ficará registado como visitado e, após uma determinada percentagem dos conteúdos aquele ponto visitado o próprio ponto fica marcado como visitado;
- f) Pontos visitados deverão poder ser marcados como “desejo visitar fisicamente”;
- g) Com a utilização da plataforma e acedendo aos seus conteúdos, serão atribuídos aos visitantes, rankings e medalhas que lhes darão acesso a algumas funcionalidades, como os comentários, as pontuações e as propostas;
- h) Os comentários deverão poder ser reportados como impróprios pelos utilizadores e serão moderados através da plataforma de controlo.

4) Sequência de visitas (tours):

- a) Um visitante deverá poder fazer uma tour onde lhe serão apresentados os conteúdos de vários pontos em sequência;
- b) Os conteúdos a apresentar deverão poder ser selecionados ou escolhidos de forma aleatória na altura da apresentação;
- c) Deverão estar disponíveis tours pré-definidas pela equipa de gestão do projeto @MADEIRA, que o visitante poderá escolher para visualizar vários pontos relacionados por categoria ou tipo;
- d) Os visitantes poderão criar e guardar as suas próprias tours que poderão visualizar várias vezes ou partilhar com outros utilizadores.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

5) Proposta de novos pontos:

- a) Será possível entidades ou privados submeterem novos pontos de interesse na plataforma que se aprovados, passarão a fazer parte da oferta;
- b) Na proposta deverão ser submetidos conteúdos, descrições e justificação;
- c) A aprovação dos pontos sugeridos poderá ser feita administrativamente pela equipa de gestão do projeto @MADEIRA ou por votação pública, por forma a aumentar a interatividade entre a oferta turística e a população em geral.

6) Gamificação:

- a) Para incentivar o uso da Plataforma, e com isso maximizar a sua utilização e dos dados por ela fornecidos, a mesma tem uma vertente de gamificação que atribui rankings e medalhas quando os visitantes consomem os conteúdos, comentam e pontuam os locais e propõe novos pontos de interesse;
- b) Esses rankings disponibilizam funcionalidades da plataforma e darão destaque aos comentários dos utilizadores mais bem cotados.

7) Retenção dos utilizadores:

- a) Os pontos estarão ligados pelas categorias para permitir, na página de cada ponto, apresentar sugestões de outros pontos ao visitante. Esta sugestão, no caso de visitantes registados, deverá ter em conta os pontos anteriormente visitados e as categorias preferidas do visitante;
- b) Periodicamente deverá ser enviado um relatório onde será apresentada ao visitante informação sobre os pontos visitados, conquistas, o que falta para atingir uma meta entre outra informação de interesse;
- c) Se o visitante não voltar a entrar na plataforma durante um determinado período deverá ser enviado um email com propostas de pontos que pode ter interesse em visitar e novos pontos entre outra informação que incentive o utilizador a voltar à plataforma.

4. Arquitetura de Referência

A plataforma @MADEIRA deverá obedecer aos seguintes requisitos:

- Os dados deverão ser alojados e mantidos nos sistemas que se encontram no âmbito deste concurso;
- A plataforma deverá ser desenvolvida numa arquitetura de alta disponibilidade;
- A plataforma deverá ser desenvolvida de forma a ser acedida via Web a partir de qualquer dispositivo, sendo os vários sistemas alojados nos sistemas objeto deste concurso;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- A aplicação deverá ser desenvolvida com base numa arquitetura de módulos independentes que garantam a fácil escalabilidade;
- As interfaces deverão ser desenvolvidas com base em modelos aprovados pela entidade gestora do projeto @MADEIRA.

5. Modelo de Gestão do Projeto

Os serviços constantes nesta cláusula deverão obedecer a um modelo de gestão que garanta a aplicação prática de uma metodologia de gestão de projeto baseada no PMBoK versão 5.

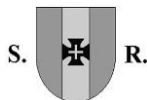
A Equipa que implementará o modelo de gestão será constituída por elementos da entidade gestora do projeto @MADEIRA e pelo fornecedor, e deve incluir:

- a) Direção de Projeto: Esta equipa deverá envolver as equipas de Direção de Projeto e demais participantes que se considere relevantes;
- b) Gestão de Projeto, que deverá incluir a equipa de Arquitetos da Solução, e cujas principais responsabilidades serão:
 - a) monitorizar a execução do plano de trabalho,
 - b) documentar e promover a documentação de todos os aspetos da projeto e solução, e
 - c) formalizar e promover as aceitações dos produtos que constituem a solução.

O Modelo de gestão do projeto deverá cobrir as seguintes áreas:

- a) Gestão de Risco;
- b) Identificação de Fatores Críticos de Sucesso;
- c) Gestão de Conformidades;
- d) Definição de Requisitos.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Secção IV – Requisitos para a Prestação de Serviços

Cláusula 35.^a

Requisitos da Componente de Serviços de Suporte e Manutenção

1. O suporte em causa é referente a atualizações dos bens, designadamente updates ou upgrades, dependendo da política do fabricante para o produto, durante o período contratado.
2. Os serviços de suporte descritos nesta cláusula dizem respeito às componentes de computação, armazenamento, proteção de dados, solução de Ciber-Resiliência, Comunicações LAN e segurança de Perímetro.
3. Os serviços de suporte e manutenção deverão ser prestados durante o período de 3 anos após assinatura do contrato.
4. A forma de comunicação deverá ser presencial, telefónica, portal ou assistência remota.
5. Os serviços de suporte remotos e on-site devem ser realizados por técnicos certificados dos fabricantes, nativos ou fluentes em língua portuguesa.
6. De forma a atestar o cumprimento do requisito anterior, deverá ser apresentada uma declaração dos fabricantes dos produtos constante na proposta, assinada pelo seu representante legal, atestando que os serviços de suporte remotos e on-site serão realizados por técnicos certificados dos fabricantes, nativos ou fluentes em língua portuguesa.
7. De forma a garantir os serviços de suporte, as entidades adjudicatárias deverão disponibilizar um serviço baseado na Web e de atendimento telefónico que deverão assegurar:
 - a) Contactos telefónicos específicos;
 - b) O registo com um identificador único de qualquer pedido de intervenção comunicado ao serviço de assistência;
 - c) Disponibilidade do serviço e tempo de resposta é de 24 x 7 x 365 dias.
8. O suporte técnico dos bens em causa que neste caso é hardware deverá incluir:
 - a) O fornecimento de peças de substituição e consumíveis para os produtos de hardware deverão ser do fabricante da solução;
 - b) As atualizações tecnológicas de programas (lógicos), consistentes nas versões subsequentes dos programas que o fabricante disponibiliza e entregues em suporte físico ao cliente ou disponibilizadas para download no endereço de internet fornecido ao cliente;
 - c) Atualizações fiscais, legais e reguladoras;
 - d) Instalação de fixes e correções para programas;
 - e) Patches de segurança;
 - f) Alertas de segurança;
 - g) Ferramentas de atualização;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- h) Certificação com novos produtos / versões de terceiros;
- i) Versões importantes de produtos e tecnologia para firmware e software de sistemas que incluem:
 - o versões de manutenção geral;
 - o Versões de funcionalidade selecionadas e atualizações de documentação.
- j) Certificação do hardware.

Cláusula 36.^a

Requisitos da Componente de Serviços de Instalação, Configuração e Formação

1. Os serviços de instalação e configuração dos equipamentos propostos, devem ser realizados on site por técnicos certificados pelos fabricantes dos equipamentos, nomeadamente das seguintes componentes da solução:
 - a) Computação
 - b) Armazenamento
 - c) Rede Local - LAN
 - d) Solução de Backups
 - e) Solução de Ciber Resiliência
 - f) Segurança Perímetro
 - g) Rede Local - Routing
2. Para cada uma das componentes deverão ser incluídas as seguintes fases macro de instalação e configuração:
 - a) Elaboração de Lista de Requisitos Técnicos de Instalação;
 - b) Reunião de Kick-Off com a entidade gestora do projeto @MADEIRA do Governo Regional da Madeira, para apresentação das equipas, discussão de plano de projetos e identificação de tarefas e respetivos responsáveis;
 - c) Apresentação de Plano de Projeto Macro;
 - d) Instalação Física dos equipamentos em Rack;
 - e) Startup dos equipamentos;
 - f) Configuração de acordo com Best Practices do fabricante e dos Requisitos Técnicos elaborados em conjunto com a equipa técnica da entidade gestora do portal @MADEIRA do Governo Regional da Madeira;
 - g) Realização de Testes de Funcionalidades, de acordo com Lista de Testes elaborada em conjunto com a equipa técnica da entidade gestora do projeto @MADEIRA do Governo Regional da Madeira;
 - h) Produção de documentação sobre arquitetura implementada, configurações e parametrização realizada;
3. Formação e Acompanhamento





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Deverão ser apresentados serviços de Formação e Acompanhamento, designadamente:

- a) Formação Training-In-The-job, para operação da solução de forma autónoma, por parte da equipa técnica da entidade gestora do projeto @MADEIRA do Governo Regional da Madeira;
- b) Formação Certificada dos Fabricantes, sendo a mesma realizada presencialmente para, pelo menos, 4 recursos da entidade gestora do projeto @MADEIRA a indicar pela entidade adjudicante;
- c) Serviços de Acompanhamento após entrada em produção (local ou remoto), de pelo menos 1/2 dia por semana, durante primeiro ano de funcionamento, para as componentes acima mencionadas.

4. Recursos:

- a) Todos os serviços constantes na presente cláusula deverão ser realizados on site por técnicos certificados dos fabricantes, nativos ou fluentes em língua portuguesa;
- b) As propostas deverão designar os recursos afetos ao projeto, devendo ser apresentado o seu Curriculum Vitae;
- c) Deverá ser apresentada uma declaração dos fabricantes, assinada pelos seus representantes legais, discriminando os recursos designados por estes para a execução do projeto;
- d) O projeto definido na presente cláusula deverá ter designado um Gestor de Projeto Certificado para garantir a correta execução das tarefas, servindo como interlocutor privilegiado com a entidade gestora do projeto @MADEIRA.

Cláusula 37.^a

Requisitos da Componente de Serviços de Desenvolvimento e Suporte Aplicacional

Local de Prestação do Serviço e Constituição da Equipa

- 1. Os serviços referentes constantes do presente caderno de encargos serão prestados nas instalações a designar pela entidade gestora do projeto @MADEIRA do Governo Regional da Madeira, sitas no Funchal, ou em regime de teletrabalho, caso se venha a revelar necessário.
- 2. Os serviços a prestar no âmbito do projeto @MADEIRA serão prestados 8 horas por dia, 5 dias por semana, podendo ser prestado, em caso de necessidade e a pedido da entidade pública adquirente, em horário pós-laboral e em dias não úteis.
- 3. O adjudicatário, para a prestação dos serviços no âmbito do projeto, obriga-se a apresentar, uma equipa constituída obrigatoriamente pelos seguintes perfis:
 - a) Coordenador de Projeto:
 - Formação académica, a nível de curso superior, nas áreas de Informática, ou Engenharia Eletrotécnica, ou Sistemas de Informação, ou Gestão de Sistemas de Informação, ou Matemática;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- Experiência na implementação de projetos tecnológicos, designadamente sistemas de informação com vertente de coordenação técnica e funcional do projeto, na componente de desenvolvimento de software, com o mínimo de 5 anos.
 - Experiência em gestão de equipas, com o mínimo de 3 anos;
 - Experiência em implementação de projetos de desenvolvimento e de manutenção de software, utilizando a tecnologia de desenvolvimento Microsoft.net designadamente Linguagem C# e Base de Dados (BD) SQL Server, com o mínimo de 5 anos;
 - Formações específicas: Power BI and Machine Learning, Business Analysis, NET Framework Developing Modern Web Apps with ASP.NET MVC (DEV - ASP.NET), Data Analyst
- b) Programador Sénior:
- Formação académica, a nível de curso superior, nas áreas de Informática, ou Engenharia Eletrotécnica, ou Sistemas de Informação, ou Gestão de Sistemas de Informação, ou Matemática;
 - Experiência em implementação de projetos de desenvolvimento e de manutenção de software, utilizando a tecnologia de desenvolvimento Microsoft.net designadamente Linguagem C# e Base de Dados (BD) SQL Server, com o mínimo de 3 (três) anos.
4. No prazo de 3 (três) dias após a entrada em vigor do contrato o cocontratante tem de apresentar a lista dos elementos que compõe a equipa, bem como respetivos currículos e/ou documentos que comprovem as habilitações académicas e demais formações e certificações, de acordo com as especificações contantes do número anterior, para ser aprovada pelo contraente público.
 5. O contraente público reserva-se ao direito de recusar elementos da equipa, apresentados pelo cocontratante, sempre que comprovadamente se verificar que não cumprem o previsto no n.º 1, da presente cláusula.
 6. No prazo de 10 (dez) dias após a entrada em vigor do contrato, se a lista dos elementos que compõe a equipa, de acordo com as especificações contantes do n.º 1 da presente cláusula, não estiver totalmente constituída e aprovada pelo contraente público, serão aplicadas as penalidades previstas no caderno de encargos. Se após este prazo a equipa ainda não se encontrar concluída o contraente público reserva-se ao direito de resolver o contrato.
 7. A equipa aprovada deverá manter-se durante toda a execução do contrato. Na eventualidade da necessidade de substituição de algum elemento que a compõe, carece de prévio acordo do contraente público devendo o cocontratante apresentar um elemento com valências equivalentes ao do substituído, bem como os documentos referentes ao novo recurso mencionado no n.º 2.
 8. Caso algum elemento da equipa aprovada quiser terminar o contrato de trabalho deverá o contraente público deverá ser informada pelo cocontratante com 30 (trinta) dias de antecedência, devendo ainda





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- o cocontratante garantir um período de sobreposição de 15 (quinze) dias entre o elemento que rescindir o contrato e o elemento que o virá substituir, para transferência de conhecimento.
9. Os elementos que compõem a equipa são colaboradores do cocontratante, que dele dependerão exclusivamente, quer jurídica, quer economicamente, recebendo do mesmo ordens e instruções referentes à boa prestação dos serviços.
 10. O planeamento e gestão dos recursos afetos à prestação dos serviços são da responsabilidade do cocontratante.
 11. Em caso de algum elemento da equipa, adotar quaisquer comportamentos que de alguma forma, lesem perturbem o ambiente de trabalho ou prejudiquem a imagem do contraente público, o cocontratante deverá proceder à sua substituição por outro elemento com idêntico perfil/experiência profissional, no prazo máximo de 5 (cinco) dias úteis.
 12. O cocontratante assume a responsabilidade por si e pelos elementos da equipa pela perfeita adequação dos trabalhos a realizar aos fins a que se destinam.
 13. O cocontratante não pode alterar unilateralmente a composição da equipa afeta à execução dos serviços, sob pena de resolução do contrato e aplicação de penalidades, conforme previsto no caderno de encargos.
 14. O cocontratante assume integral responsabilidade pelos serviços contratados, sendo o único responsável perante o contraente público pela boa prestação dos mesmos.
 15. É da exclusiva responsabilidade do cocontratante o cumprimento das obrigações legais e regulamentares relativas aos elementos afetos à prestação de serviços, nomeadamente no que concerne ao registo de pessoal, aptidão profissional, condições de trabalho, organização do tempo de trabalho, disciplina, bem como o respeito pela legislação e regulamentação coletiva aplicável, incluindo a que respeita os direitos e garantias conferidos aos recursos humanos, ressaltando-se os referentes a remuneração, proteção da segurança e saúde e assistência em caso de doença ou acidente de trabalho.
 16. O cocontratante responde por quaisquer erros, deficiências ou omissões na prestação de serviços, qualquer que seja a sua origem e/ou o momento em que forem detetados, salvo se aquele provar que os mesmos decorreram de dados fornecidos por escrito pelo contraente público.
 17. As ações de supervisão e controlo por parte do contraente público em nada alteram ou diminuem a responsabilidade do cocontratante no que se refere à sua prestação dos serviços.
 18. Em caso de falta de algum dos recursos alocados à prestação dos serviços, deverá o cocontratante assegurar a sua substituição imediata, de modo a garantir a correta execução dos serviços contratados, reservando o contraente público ao direito previsto o n.º 3 da cláusula anterior.
 19. Caso o cocontratante não assegure a substituição do recurso alocado, no prazo máximo 2 (duas) horas contadas desde o prazo fixado para início da execução dos serviços diários, será considerado um dia completo, para efeitos de aplicação das penalidades previstas no caderno de encargos.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

20. Não obstante a aplicação de penalidades nos termos do número anterior, todas as horas de serviço não executadas deverão ser compensadas de acordo com as indicações do contraente público.
21. Em qualquer dos casos previstos nos números anteriores, deverá o cocontratante reportar imediatamente a situação ao contraente público, na pessoa responsável pela monitorização do contrato.

Requisitos dos Serviços de Manutenção Corretiva e Preventiva

1. O cocontratante para assegurar a análise, desenho, programação, testes e implementação de novos módulos, deve obrigatoriamente cumprir as seguintes tarefas:
 - a) Análise e documentação dos módulos a desenvolver;
 - b) Desenho técnico, programação e testes;
 - c) Planeamento de cronograma de desenho, desenvolvimento, teste e implementação;
 - d) Implementação em produtivo dos módulos a desenvolver.
 - e) Planos de Testes;
 - f) Elaboração de documentação de controlo de configuração e versionamento.
2. O cocontratante obriga-se durante a duração do contrato, e nos termos definidos no caderno de encargos, a assegurar toda a componente de Manutenção Preventiva visando assegurar a análise, desenho, programação, testes e implementação de melhorias, para otimização de processos, para garantir a qualidade dos dados dos sistemas e incorporar alterações legislativas que venham a decorrer durante os projetos, tendo como principais tarefas:
 - a) Análise e documentação de melhorias;
 - b) Análise de impacto no sistema existente;
 - c) Análise dos processos de melhoria da qualidade dos dados dos sistemas;
 - d) Desenho técnico, programação e testes;
 - e) Implementação em produtivo da melhoria;
 - f) Apoio na eventual migração de dados;
 - g) Produção de testes de verificação de níveis de serviço;
 - h) Acompanhamento de indicadores de níveis de serviço;
 - i) Estabelecer padrões de desempenho e limites de alerta;
 - j) Proceder a verificação e otimização de recursos ocupados.
3. O cocontratante obriga-se durante a duração do contrato, e nos termos definidos no presente caderno de encargos, a assegurar toda a componente de Manutenção Corretiva, visando identificar, documentar e corrigir eventuais anomalias que se venham a detetar durante o projeto, tendo como as principais tarefas:
 - a) Análise e documentação de anomalias detetadas;
 - b) Análise de impacto para correção das anomalias;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- c) Análise de medidas de implementação de processos de melhoria da qualidade dos dados;
 - d) Correção e testes das anomalias;
 - e) Documentação das correções de controlo de configuração;
 - f) Testes de regressão das funcionalidades principais após correções;
 - g) Produção de procedimentos de recuperação em emergência;
 - h) Implementação em produtivo da funcionalidade corrigida.
4. Na manutenção corretiva do software aplicacional será feita a correção a todos os erros de programação, bem como todas as situações não conformes com o caderno de encargos e eventuais inconsistências na documentação.
5. Com o objetivo de assegurar que eventuais erros nos sistemas não impactem na operacionalidade dos serviços do contraente público, a gestão das ocorrências dos sistemas sujeitas a manutenção corretiva, deverá ser cumprir o seguinte workflow:
- a) As correções são despoletadas por relatórios de ocorrências, a entregar pelo contraente público, através de *email*, telefone ou através do *Help Desk*, ao cocontratante, na figura do Coordenador do projeto.
 - b) Após a receção destes relatórios de ocorrências é feita a análise por parte do cocontratante, para que seja determinado se o problema é da aplicação ou de operação.
 - c) No primeiro caso, o relatório é entregue diretamente ao programador designado ao sistema em causa.
 - d) No segundo caso, o Coordenador contacta com quem reportou o problema para o informar do modo correto de operação ou para prestar esclarecimentos adicionais.
 - e) Todas as correções deverão ser colocadas no Ambiente de Testes/Qualidade do contraente público de modo a serem efetuados testes, antes de serem colocadas em produção.
 - f) Após a correção da situação, o Coordenador informará quem despoletou o processo da resolução do problema.
6. A equipa de manutenção do software aplicacional será responsável por manter guardadas todas as versões do sistema, com o respetivo conjunto de testes, utilizando um software específico para esse propósito. Todas as versões poderão ser auditadas e consultadas pelo contraente público, sempre que este o solicitar. O contraente público terá sempre a capacidade de efetuar o controlo da manutenção corretiva através de:
- a) Controlo de Ocorrências;
 - b) Testes e/ou alarmes de desempenho aplicacional;
 - c) Controlo de Atualizações das Aplicações.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

Cláusula 38.^a

Requisitos da Componente de Serviços de Administração de sistemas

1. A equipa de Administração de Sistemas será responsável por garantir o bom funcionamento da infraestrutura tecnológica e software base que suporta a solução @MADEIRA. Deverão estar incluídas, mas não só, as seguintes tarefas:
 - a) Instalação de novo Hardware;
 - b) Upgrade de BIOS ou Patchs nos sistemas de Hardware;
 - c) Instalação, upgrade ou aplicação de patchs em sistemas Operativos;
 - d) Instalação, upgrade ou aplicação de patchs em software de bases de dados e similares;
 - e) Gestão de hipervisors, que inclui upgrades e patchs, criação e gestão de máquinas virtuais, gestão de clusters, etc;
 - f) Gestão de sistemas de armazenamento, que inclui, mas não só, upgrades de firmware, upgrades de software, criação de LUNs, Gestão de Acessos;
 - g) Gestão de Backups, que inclui, mas não só, execução de cópias de segurança, testes de recuperação, etc;
 - h) Gestão do sistema de Ciber-resiliência, que inclui, mas não só, análise de logs, análise de reports, garantia de aplicação dos últimos patchs ou upgrades, testes de integridade, etc;
 - i) Gestão de redes, que inclui definição de regras de segurança e reencaminhamento, definição de vLANS, etc;
 - j) Gestão do sistema de segurança de perímetro, que inclui definição de regras de segurança, análise continua, etc.
2. A Equipa de administração deverá incluir, no mínimo os seguintes elementos:
 - a) Um coordenador de equipa com o mínimo de 5 (cinco) anos de experiência em funções similares;
 - b) Um técnico especialista na plataforma tecnológica de computação com pelo menos 2 (dois) anos de experiência;
 - c) Um técnico especialista na plataforma de hipervisors com pelo menos 2 (dois) anos de experiência;
 - d) Um técnico especialista na plataforma tecnológica de armazenamento com pelo menos 2 (dois) anos de experiência;
 - e) Um técnico especialista na plataforma tecnológica de Proteção de Dados e Ciber-resiliência com pelo menos 2 (dois) anos de experiência;
 - f) Um técnico especialista na plataforma tecnológica de Segurança de Perímetro com pelo menos 2 (dois) anos de experiência;
 - g) Todos os recursos devem ser certificados pelo Fabricante do Hardware ou Software para administração e gestão dos sistemas, devendo ser apresentada uma declaração do(s)





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

fabricante(s), assinadas pelo seu representante legal, identificando o técnico e as certificações que este possui.

3. Será responsabilidade da equipa de administração garantir a interlocução entre as várias partes, nomeadamente Call Center, equipas de suporte dos fabricantes, elementos designados pela entidade de gestão do projeto @MADEIRA.
4. Será responsabilidade da equipa de administração apresentar um relatório mensal indicando:
 - a) Ações solicitadas;
 - b) Ações Efetuadas;
 - c) Erros e Avarias reportados;
 - d) Erros e Avaria resolvidos;
 - e) Relatórios de boa execução de cópias de segurança;
 - f) Relatórios de execução de testes de recuperação;
 - g) Ameaças e Tentativas de intrusão detetadas pelo sistema de defesa de perímetro;
 - h) Ações efetuadas para defesa;
 - i) Impacto da tentativa de intrusão;
 - j) Ações preventivas efetuadas (patches, upgrades, etc);
 - k) Ações planeadas;
 - l) Downtimes totais ou parciais passados e previstos;
 - m) Sugestões de melhoria continua.
5. Os serviços de administração deverão ser realizados 7 dias por semana com cobertura de 24h por dia.
6. A equipa de administração de sistemas deverá estar localizada nas instalações a designar pela entidade gestora do portal @MADEIRA, sita no Funchal.
7. Deverá ser disponibilizada uma linha de atendimento por telefone ou mail para registo de pedidos.
8. Os pedidos efetuados à equipa de administração deverão ser respondidos no prazo máximo de 2 (duas) horas após abertura da chamada.
9. Os serviços de administração deverão ser garantidos durante um período de 2 (dois) anos, a contar após assinatura da aceitação do projeto.

Cláusula 39.^a

Requisitos da Componente de Alojamento e Comunicações

1. Deverá ser garantido um serviço de Alojamento da Plataforma Tecnológica de suporte ao @MADEIRA.
2. O serviço de alojamento deverá garantir:
 - a) Alimentação elétrica ininterrupta e redundante;
 - b) Sistemas de arrefecimento ininterruptos e redundantes;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

- c) Links redundantes de acesso à Internet com pelo menos 2Gpbs garantidos de largura de banda;
 - d) Sistema de Controlo de Acessos que permita somente a operadores autorizados que acedam aos bastidores onde se encontra a plataforma tecnológica de suporte ao @MADEIRA.
3. Deverá ser garantido o acesso remoto aos sistemas por parte da Equipa de Administração de Sistemas de forma que estes possam de forma ininterrupta desempenhar as suas funções.
 4. Deverá ser garantido o acesso físico aos sistemas por parte da Equipa de Administração de sistemas para a realização de tarefas que não possam se realizadas de forma remota.
 5. O Centro de Dados deverá estar colocado na Região Autónoma da Madeira de forma a assegurar o continuo acesso aos sistemas.
 6. O Serviço de Alojamento e Comunicações deverá ser prestado durante o período de 3 (três) anos a contar a partir da assinatura do auto de aceitação.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

ANEXO I – CONSULTA PRELIMINAR AO MERCADO

A Direção Regional de Informática, com vista à preparação do presente procedimento aquisitivo, e fazendo uso do disposto no artigo 35.º-A do CCP, procedeu nos termos da denominada “Consulta Preliminar ao Mercado” à solicitação de informação a operadores económicos, nos seguintes termos:

I - Objeto do contrato a celebrar

Aquisição de serviços de desenvolvimento da plataforma @MADEIRA e respetiva base tecnológica de suporte

II - Informação pretendida

A informação pretendida, para além da considerada pelo operador económico como oportuna e relevante, deverá abordar os seguintes aspetos:

- **Identificação do operador económico:** nome, endereço, contactos;
- **Informação financeira com vista a formar o preço base do procedimento aquisitivo:** Preço de venda dos bens e serviços melhor caracterizados no anexo à referida consulta com as quantidades, especificações, requisitos técnicos e funcionais mínimos.

III - Modo e prazo de apresentação da consulta

A prestação voluntária das informações ora solicitadas, deverá ser feita através de correio eletrónico, **para o endereço aquisicoes.informatica@madeira.gov.pt, até fim do dia 28/07/2022.**

IV - Forma da consulta

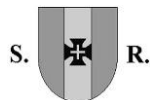
Segundo o artigo 35.º-A do CCP é imperativo que a consulta preliminar ao mercado seja conduzida com transparência e não haja tratamento desigual de operadores económicos. Tendo em conta a prossecução destes princípios, a informação da consulta preliminar constará do respetivo processo administrativo.

Configurando a Consulta Preliminar uma “auscultação” ao mercado, a presente consulta tem um caráter meramente informativo, não estando a Direção Regional de Informática vinculada às informações prestadas pelos operadores económicos, pelo que as mesmas poderão não ser consideradas nas peças do procedimento de formação do contrato a aprovar pelo órgão competente para a decisão de contratar.

Nesta conformidade, **a 22/07/2022 foram consultados** os seguintes operadores económicos:

1. PAMAFE IT - Informática, Lda;
2. DELL Technologies;





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
DIREÇÃO REGIONAL DE INFORMÁTICA

3. Link Consulting.

Findo o prazo estipulado para a apresentação voluntária das informações então solicitadas, concluiu-se que os seguintes operadores económicos **acederam à consulta preliminar**:

1. PAMAFE IT - Informática, Lda;
2. DELL Technologies;
3. Link Consulting.

