



**Chamada de Oportunidade de Serviços de Nuvem Pública Nº. 011/2021, aderente
ao Edital de Pré-qualificação Permanente de Serviços em Nuvem Nº 001/2019 -
ETICE**

Dezembro de 2021

1. OBJETO

Chamada de oportunidade para Serviços de Provimento de Sistemas para Nuvem.

2. OBJETIVOS:

Contribuindo com o aprimoramento tecnológico dos entes da Administração Pública do Estado do Ceará e reforçando sua missão de ser referência nacional como empresa de Tecnologia da Informação e Comunicação – TIC, indutora da inovação e modernização para o desenvolvimento econômico-social no fornecimento de serviços de tecnologia de alta performance em nuvem, a **ETICE** deseja selecionar, dentre as empresas pré-qualificadas, **serviços técnicos especializados para provimento de solução em nuvem**, conforme detalhamento técnico constante neste documento.

Assim, considerando as premissas estabelecidas no Edital de Pré-qualificação 001/2019, a Empresa de Tecnologia da Informação do Ceará – ETICE convoca as empresas pré-qualificadas para **que apresentem propostas para fornecimento dos serviços em nuvem, seguindo as definições técnicas deste documento convocatório.**

Todos os recursos e serviços necessários deverão ser lançados na proposta em modalidade OPEX.

Outrossim, vale destacar que os itens de serviços vencedores de cada chamada de oportunidade já serão trazidos para a composição do Marketplace da ETICE, devendo o(s) contrato(s) serem realizados por demanda; ou seja, **SEM** comprometimento do Orçamento da ETICE, podendo haver a contratação parcelada do objeto da presente chamada de Oportunidade; tudo consoante ao disposto nos itens 13.11, 17.1.1, 17.1.2 e 17.1.3 do Edital de Préqualificação, *in verbis*:

“13.11. Os itens de serviços vencedores de cada chamada de oportunidade serão trazidos para a composição dos serviços do marketplace da Etice, devendo seus preços finais serem mantidos como máximos por um prazo mínimo de 12 (doze) meses a contar da data da homologação do resultado da chamada de oportunidade.

(...)

17.1.1. Consoante o disposto no art. 140, parágrafos 4º e 5º do Regulamento de Licitações e Contratos da Etice, **fica desde já a ETICE autorizada a celebração de contratos por demanda.**

17.1.2. A ETICE fixará um quantitativo ou valor máximo de fornecimento ou serviço a ser utilizado no prazo de vigência do referido contrato, **SEM comprometimento do Orçamento da Etice.**

17.1.2. Na hipótese do item anterior, a ETICE **demandará o objeto de forma PARCELADA e apenas quando necessitar, nos termos e prazos definidos no Edital e contrato, remunerando o contratado apenas pelo que for efetivamente executado.**” (grifou-se)

Este documento descreve as **características funcionais, premissas técnicas e de serviços** que deverão ser consideradas pelas pré-qualificadas, para que, munidos de informações relevantes sobre as necessidades para atendimento ao escopo dos serviços, emitam propostas de acordo com as condições preestabelecidas no Edital de Pré-qualificação supracitado.

3. SOBRE O MODELO DE CONTRATAÇÃO

3.1 Esta chamada de oportunidade obedecerá ao disposto no **Edital de pré-qualificação de nuvem nº 001/2019 da ETICE e seus anexos, nos Termos de Pré-Qualificação e no Regulamento de Licitações e Contratos da ETICE**; sendo regido, também, pela **Lei Federal 13.303/2016, pelos Princípios do Direito Civil e, no que couber, pelos Princípios da Administração Pública e demais legislação correlata.**

3.2 A chamada será feita em lote único visto que os itens desta chamada são intrinsecamente interconectados o que impossibilitaria sua divisão.

3.3 Justificativa de escolha da padronização do VMWare e Microsoft Server:

3.3.1 Considerando a quantidade de demanda de clientes ETICE para utilização dos software de Nuvem VMWare e Microsoft Server;

3.3.2 Considerando que grande parte do parque já instalado no Estado utiliza VMWare e Microsoft Server;

3.3.3 Considerando que tanto o VMWare como o Microsoft Server são classificados como líderes no quadrante mágico do Gartner em suas respectivas categorias.

3.3.4 Considerando que todos os CSPs podem ofertar essa padronização.

3.3.5 Assim sendo, a presente chamada de oportunidade usará a padronização de diversos componentes do VMWare necessários para nuvens e Microsoft Server.

4. ORIENTAÇÕES GERAIS

4.1 Prazos

Número do Evento	Evento	Prazo limite
1	Recebimento de propostas das empresas pré-qualificadas pela ETICE	8 (oito) dias úteis (*)
2	Pedidos de Esclarecimentos	<u>Até às 17h:00min do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.</u>
3	Resposta aos Pedidos de	Até 2 (dois) dias úteis, a contar do término do prazo

	Esclarecimentos	de pedidos de esclarecimentos (**).
4	Pedidos de Impugnação	Até às 17h:00min do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.
5	Respostas à Impugnação Interposta	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimento.
6	Avaliação e classificação dos candidatos a proposta vencedora pela ETICE, com convocação do primeiro candidato classificado para apresentar documentação de habilitação e características técnica da solução proposta	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de propostas
7	Prazo para responder a convocação para apresentar documentação técnica	Até 02 (dois) dias úteis após ser convocado
8	Prazo para análise e definição de proposta vencedora ou convocação de novo candidato para apresentar documentação técnica	Até 05 (cinco) dias úteis após receber a documentação do candidato (**)
9	Interposição de Recurso	Até 5 (cinco) dias úteis, contados a partir da divulgação da proposta vencedora.
10	Apresentação de Contrarrazões ao Recurso	Até 5 (cinco) dias úteis, contados a partir do término do prazo de interposição de recurso.
11	Decisão definitiva da Comissão	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de contrarrazões recursais, podendo variar em razão da complexidade da matéria.

12	Homologação e Adjudicação	Até 5 (cinco) dias úteis, a contar da divulgação da decisão definitiva da Comissão.
----	---------------------------	---

(*) O prazo será contado a partir do primeiro dia útil seguinte à publicação deste documento no website da ETICE, no link <https://www.etice.ce.gov.br/projeto/pre-qualificacao-permanente/>.

(**) O prazo poderá ser alterado conforme disposto no item 5.4.

(***) Caso haja desistência expressa do Prazo Recursal (e consequente Contrarrazões), o Prazo para apresentação da Decisão Definitiva poderá ser reduzido, conforme o caso.

- 4.1.1 Os Prazos dispostos no item acima poderão variar em conformidade com o caso concreto, podendo inclusive serem mitigados, em razão de não apresentação de recursos ou mesmo que as empresas Pré-qualificadas declinem, formalmente, do direito Recursal (e consequentemente das Contrarrazões).

4.2 Sobre o envio da Proposta Técnicas

- 4.2.1 Em razão do período delicado de Pandemia mundial que estamos passando, e até mesmo como um mecanismo de evitar o trânsito de papel e aglomeração de pessoas, consoante previsão disposta no item 13.8.2 do Edital nº, 001/2019 de Pré-Qualificação, a proposta deverá ser enviada de **forma eletrônica** e deverá inicialmente ser **CRIPTOGRAFADA** utilizando o algoritmo de criptografia AES-256 (FIPS PUB 197).
- 4.2.2 O proponente é responsável por gerar uma chave aleatória de 256 bits e **manter completo sigilo desta chave, sem revelá-la a terceiros, nem à Etice**, até que se tenha passado o período de recebimento de propostas estabelecido na tabela do item 6.1.
- 4.2.3 Antes ou após criptografada utilizando-se o algoritmo AES-256, a proposta deve ser assinada digitalmente, conforme o modelo da Medida Provisória 2.200-2/2001.
- 4.2.3.1 Com o objetivo de facilitar a submissão de propostas e considerando que vários *softwares* possibilitam a assinatura digital de um documento antes de uma encriptação e não após ela a ETICE aceitará também propostas que tenham sido assinadas digitalmente antes de terem sido encriptadas contanto que o nome do arquivo de proposta possibilite a identificação clara do proponente.
- 4.2.4 A proposta criptografada e assinada deve ser enviada para o e-mail avaliacao.nuvem@etice.ce.gov.br. **O HORÁRIO DE RECEBIMENTO DAS PROPOSTAS SERÁ ATÉ ÀS 17H (DEZESSETE HORAS) DO ÚLTIMO DIA ÚTIL PARA RECEBIMENTO DAS PROPOSTAS.**

- 4.2.5 Uma proposta só será considerada entregue no prazo caso a Etice responda com um e-mail para o proponente reconhecendo o recebimento dentro do prazo.
- 4.2.6 A resposta da Etice será assinada digitalmente ou de outra forma por ela estabelecida.
- 4.2.7 Proposta enviada para e-mail não correto ou com erro de escrita ou que tenha sido recusado pelo servidor não serão considerados entregues no prazo.
- 4.2.8 A proponente deverá enviar a chave criptográfica usada para encriptar a proposta com o algoritmo AES-256 para a Etice em até 12 (doze) horas após encerrado o prazo de recebimento de propostas.
- 4.2.9 Arquivos corruptos ou chaves que não permitam descriptografar a proposta, farão a proposta nula.
- 4.2.10 **Todos os recursos e serviços necessários deverão ser lançados na proposta em modalidade OPEX e em moeda nacional (reais).**
- 4.2.11 Na proposta deverá constar as cotações de todos os itens de serviços especificados neste documento, expressas em reais e em valores mensais e anuais.
- 4.2.12 Para fins de elaboração de Proposta, as empresas participantes deverão considerar que o prazo contratual será de 12 (doze) meses, prorrogável na forma da lei.
- 4.2.13 A Etice descriptografará todas as propostas válidas e ordenará tais propostas baseadas em seu valor global.

5 ESCLARECIMENTOS

- 5.1 As dúvidas na interpretação do presente documento e anexos, consultas ou pedido de esclarecimentos acerca das informações técnicas porventura existentes, poderão ser feitos via e-mail de forma **expressa, clara, concisa e objetiva**, constando no corpo do texto do e-mail a identificação completa da empresa pré-qualificada participante e do representante que questiona as informações ou solicita esclarecimentos.
- 5.2 Os pedidos de esclarecimentos deverão ser encaminhados até às 17h:00min do 3º (terceiro) dia útil que antecede o término do prazo de apresentação das propostas.
- 5.3 O endereço de e-mail para os esclarecimentos é: avaliacao.nuvem@etice.ce.gov.br.
- 5.4 A Etice terá um prazo de até 02 (dois) dias úteis para resposta, sendo possível estender esse prazo de acordo com a complexidade dos esclarecimentos e/ou a necessidade de utilização de recursos técnicos externos à Etice.
- 5.5 Caso a(s) resposta(s) dos esclarecimentos provoquem alterações das definições técnicas do projeto e estas sejam consideradas relevantes pela Etice,

será reiniciada a contagem dos prazos estabelecidos no item 6.1 deste documento, cabendo comunicação prévia e única a todas as pré-qualificadas.

- 5.6** As quantidades aqui mencionadas são previsões e não implicam em obrigatoriedade de contratação de quaisquer quantidades pela Administração Pública, servindo apenas como referencial para a elaboração das propostas das empresas pré-qualificadas pela ETICE.

6 ESPECIFICAÇÃO TÉCNICA DOS SERVIÇOS

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE
1	Cessão de direito de uso de Software de Proteção de Dados para Nuvem	LICENÇA	100
2	Cessão de direito de uso de Software de Firewall para Nuvem	LICENÇA	40
3	Cessão de direito de uso de Software de Microsoft Server Data Center para Nuvem	LICENÇA	300
4	Cessão de direito de uso de Software de VMware vSphere Enterprise Plus para Nuvem	LICENÇA	40
5	Cessão de direito de uso de Software de VMware vRealize Cloud Universal Advanced para Nuvem	LICENÇA	40
6	Cessão de direito de uso de Software de VMware vRealize Cloud Universal Enterprise para Nuvem	LICENÇA	40
7	Cessão de direito de uso de Software de VMware NSX Data Center Advanced para Nuvem	LICENÇA	40
8	Cessão de direito de uso de Software de VMware VCenter para Nuvem	LICENÇA	5
9	Serviços de gerenciamento, orquestração da nuvem, sustentação, administração dos projetos.	UST	30.000

6.1 Especificação Detalhada:

- 6.1.1 ITEM 1 - Cessão de direito de uso de Software de Proteção de Dados para Nuvem
 - 6.1.1.1 O Software de proteção de dados disponibilizará licenças para proteção de dados em Nuvem.
 - 6.1.1.2 A Solução de proteção de dados deve ter as características técnicas conforme item 1 do Anexo A.
- 6.1.2 ITEM 2 - Cessão de direito de uso de Software de Firewall para Nuvem
 - 6.1.2.1 O Software de Firewall para Nuvem disponibilizará licenças para firewall de Nuvem.
 - 6.1.2.2 O Software de Firewall para Nuvem Privada deve ter as características técnicas conforme item 2 do Anexo A.
- 6.1.3 ITEM 3 - Cessão de direito de uso de Software de Microsoft Server Data Center para Nuvem
 - 6.1.3.1 O Software Microsoft Server Data Center disponibilizará licenças “Microsoft Server Data Center para 2 cores” para servidores de Nuvem.
- 6.1.4 ITEM 4 - Cessão de direito de uso de Software de VMware vSphere Enterprise Plus para Nuvem
 - 6.1.4.1 O Software VMware vSphere Enterprise Plus disponibilizará licenças “VMware vSphere Enterprise Plus per CPU” para servidores de Nuvem.
- 6.1.5 ITEM 5 - Cessão de direito de uso de Software de VMware vRealize Cloud Universal Advanced para Nuvem
 - 6.1.5.1 O Software VMware vRealize Cloud Universal Advanced disponibilizará licenças “VMware vRealize Cloud Universal Advanced per CPU” para servidores de Nuvem.
- 6.1.6 ITEM 6 - Cessão de direito de uso de Software de VMware vRealize Cloud Universal Enterprise para Nuvem
 - 6.1.6.1 O Software VMware vRealize Cloud Universal Enterprise disponibilizará licenças “VMware vRealize Cloud Universal Enterprise per CPU” para servidores de Nuvem.
- 6.1.7 ITEM 7 - Cessão de direito de uso de Software de VMware NSX Data Center Advanced para Nuvem
 - 6.1.7.1 O Software VMware NSX Data Center Advanced disponibilizará licenças “VMware NSX Data Center Advanced” para servidores de Nuvem.
- 6.1.8 ITEM 8 - Cessão de direito de uso de Software de VMware VCenter para Nuvem
 - 6.1.8.1 O Software VMware VCenter disponibilizará licenças “VMware VCenter” para servidores de Nuvem.
- 6.1.9 ITEM 9 - Serviços de gerenciamento, orquestração da nuvem, sustentação, administração dos projetos
 - 6.1.9.1 A especificação detalhada do item 9 estão descritas no Anexo B.

6.2 DO ACORDO DE NÍVEIS DE SERVIÇOS – SLA

- 6.2.1 A gestão e fiscalização do contrato se darão mediante o estabelecimento e acompanhamento de indicadores de desempenho, disponibilidade e qualidade, que comporão o Acordo de Nível de Serviço (SLA) entre a Contratante e Contratada.
- 6.2.2 Será de responsabilidade da CONTRATANTE o atendimento de 1º nível.
- 6.2.3 Os chamados de 2º e 3º níveis fora dos horários acima e em dias úteis deverão ser atendidos pelo serviço de plantão, independentemente de ser sábado, domingo ou feriado. Os chamados de plantão incorrem em uma remuneração adicional medida em Unidades de Suporte Técnico (UST).
- 6.2.4 Os incidentes, situações inesperadas e não programadas, deverão ser atendidas pelos serviços de suporte da CONTRATADA. Os incidentes têm a seguinte classificação:
- Severidade 1 ou Alta:** Ambiente/Sistema está indisponível ou usuário sem acesso;
- Severidade 2 ou Média:** Uma função do Ambiente/Sistema está indisponível;
- Severidade 3 ou Baixa:** O Ambiente/Sistema está disponível, porém apresentando lentidão, erros que forçam o reinício do sistema e/ou de operações no mesmo, e/ou alguma intermitência em seu funcionamento.
- 6.2.5 A CONTRATADA deverá prestar, durante a vigência deste contrato, serviços de suporte a produção e manutenção corretiva abrangendo no mínimo:
- 6.2.6 Investigação e resolução de problemas no ambiente, mesmo que para isso seja necessário acionar o suporte do fabricante;
- 6.2.7 Nível de serviço (SLA), para chamados abertos entre o horário compreendido entre as 08 horas e 18 horas em dias úteis, conforme tabela a seguir:

Severidade	Natureza do Problema	Tempo de Resposta
Alta	Defeitos que tem como consequência a indisponibilidade do Ambiente / Sistema da CONTRATANTE	Até 10 (dez) horas contadas após registro do chamado, para diagnóstico e solução de contorno ou definitiva.
Média	Defeitos que tem como consequência a indisponibilidade parcial do Ambiente / Sistema da CONTRATANTE	Até 20 (vinte) horas úteis após registro do chamado, para diagnóstico e solução de contorno ou definitiva.
Baixa	Defeitos que não causam indisponibilidade do Ambiente / Sistema da CONTRATANTE, porém, impedem seu uso	Até 30 (trinta) horas úteis após registro do chamado, para diagnóstico e solução

	normal	de contorno ou definitiva
--	--------	---------------------------

- 6.2.8 Caso seja necessário complemento de informações para atendimento do chamado, que impossibilitem a resolução do chamado pela CONTRATADA, a CONTRATANTE será solicitados para fornecer a informação, e os prazos serão suspensos ou prorrogados até o recebimento das informações.
- 6.2.9 O tempo em horas, previsto no SLA, será computado a partir da abertura do chamado até a sua regularização, nesse caso, uma solução de contorno poderá ser utilizada, caso a solução definitiva não seja possível de ser executada imediatamente.
- 6.2.9.1 Em caso de atendimento presencial o SLA começa a ser contado a partir da chegada do técnico no local.
- 6.2.10 **A CONTRATADA deverá atender no mínimo 90% (noventa por cento) dos chamados dentro do SLA estabelecido na tabela.**

6.3 DO PAGAMENTO

- 6.3.1 O pagamento será efetivado mensalmente mediante apresentação da fatura dos serviços efetivamente executados no período.
- 6.3.2 O gestor do contrato atestará a fatura após a verificação dos serviços relacionados.
- 6.3.3 Os preços inicialmente contratados serão reajustados após o período de um ano, contado da data limite para apresentação da proposta, utilizando-se, para tanto, o Índice Nacional de Preços ao Consumidor Amplo – IPCA.
- 6.3.4 Os reajustes subsequentes ao primeiro serão efetuados quando se completarem períodos múltiplos de um ano, contados sempre do último reajuste e do valor que passou a vigorar naquela oportunidade.
- 6.3.5 No caso de atraso ou não divulgação do índice de reajustamento será calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.
- 6.3.6 Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.
- 6.3.7 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

6.4 DO CANCELAMENTO DOS SERVIÇOS

- 6.4.1 Nos casos em que a demanda for cancelada pela Etice a execução do sistema deverá ser descontinuada.
- 6.4.2 A ETICE e seus clientes finais concordam em desinstalar o sistema contratado em até 30 (trinta) dias, ou no prazo da licença adquirida, após a solicitação de cancelamento.

6.4.3 O pagamento do sistema cessará 30 (trinta) dias, ou no prazo da licença adquirida, após a notificação da CONTRATADA desta solicitação.

7 DA VIGÊNCIA DO CONTRATO

7.1 Os prazos de vigência e de execução contratual serão de 12 (doze) meses, podendo ser prorrogado, a critério da Contratante, com concordância da contratada, por períodos iguais ou inferiores, conforme art. 71 da Lei Federal 13.303/2016.

8 DO MODELO DE PROPOSTA

8.1 O modelo de proposta encontra-se no Anexo E.

9 DA FRAUDE E DA CORRUPÇÃO

9.1 As Pré-Qualificadas devem observar e a contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.

9.1.1 Para os propósitos deste item, definem-se as seguintes práticas:

a) “**prática corrupta**”: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

b) “**prática fraudulenta**”: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

c) “**prática conluiada**”: esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

d) “**prática coercitiva**”: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando a influenciar sua participação em um processo licitatório ou afetar a execução do contrato.

e) “**prática obstrutiva**”:

(1) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista neste subitem;

(2) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

9.2 Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

- 9.3 Considerando os propósitos dos itens acima, a licitante vencedora como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.
- 9.4 A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, concluídas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

10 DA SUBCONTRATAÇÃO

- 10.1 Será admitida a subcontratação no limite de até 30% (trinta por cento) do objeto, conforme disposto no art. 78 da Lei nº 13.303/2016 e nos arts. 143 a 147 do Regulamento de Licitações e Contratos da ETICE, desde que não constitua o escopo principal da contratação, e, se previamente aprovada pela ETICE.
- 10.2 A subcontratação de que trata esta cláusula, **não exclui a responsabilidade da contratada perante a ETICE** quanto à qualidade do objeto contratado, **não constituindo, portanto, qualquer vínculo contratual ou legal da ETICE com a subcontratada.**
- 10.3 A empresa subcontratada deverá atender, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas a licitante vencedora.
- 10.4 É **vedada** a subcontratação de empresa ou consórcio que tenha participado:
- 10.4.1 Do procedimento licitatório do qual se originou a contratação.
- 10.4.2 Direta ou indiretamente, da elaboração de projeto básico ou executivo.

11 DA HABILITAÇÃO TÉCNICA E CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO

- 11.1 Em razão da complexidade da presente chamada de oportunidade, serão necessárias as comprovações adicionais, relativas às Características Técnicas da solução a ser empregada, em conformidade ao disposto nos itens 13.2 e 13.6 do Edital de Pré_ qualificação 0001/2019 –ETICE, os quais dispõem:
- “13.2. As chamadas de oportunidades apresentarão as características funcionais, especificidades, **premissas técnicas** e de serviços que deverão ser consideradas pelas préqualificadas, para que, munidas de informações relevantes sobre as necessidades para atendimento ao escopo dos serviços, emitam propostas de acordo com as condições específicas preestabelecidas em cada chamada.
- (...)
- 13.6. Nas chamadas de oportunidades poderão ser aplicadas exigências, regras e critérios em caráter eliminatório e/ou classificatório,**

caracterizando a chamada dentre as opções estabelecidas no regulamento de licitações e contratos da Etice” (Grifou-se)

- 11.2 As características técnicas da solução devem ser comprovadas por uma descrição detalhada das características técnicas dos componentes do item 1 e 2, incluindo marca e modelo (ou versão) do sistema proposto, que possibilite uma completa avaliação do mesmo. A Pré Qualificada deverá fornecer uma matriz ponto a ponto comprovando as exigências expressas neste documento, com a indicação da página do datasheet, manuais, certificação dos equipamentos e serviços que serão ofertados. A matriz de características técnicas é de preenchimento obrigatório pela Pré Qualificada.
- 11.3 O preenchimento da matriz de características técnicas deverá ser realizado baseado em documentos cuja origem seja exclusivamente do fabricante da solução, como catálogos, ou manuais, ou ficha de especificação técnica, ou informações obtidas em sites oficiais do fabricante através da Internet, indicando as respectivas URL (Uniform Resource Locator). Declarações do fabricante ou da Pré Qualificada só serão aceitas em casos que seja claro a impossibilidade de usar outro tipo de comprovação. As comprovações devem ser claras, com indicação de página. Serão aceitos documentos em português ou inglês para comprovações técnicas. A não comprovação de alguma característica exigida levará a desclassificação da proposta.
- 11.4 A Pré Qualificada deverá incluir na documentação as comprovações das especificações técnicas como folder, manuais e catálogos.

12 DAS DISPOSIÇÕES GERAIS

- 12.1 **Esta chamada de oportunidade não importa necessariamente em contratação**, nos moldes já dispostos Edital de Pré-Qualificação 001/2019, podendo a autoridade competente revogá-la por razões de interesse público, anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante decisão devidamente fundamentada, sem quaisquer reclamações ou direitos à indenização ou reembolso.
- 12.2 É facultada à Comissão de Avaliação ou à autoridade competente, em qualquer fase da licitação, a **promoção de diligência** destinada a esclarecer ou a complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos que deveriam constar originariamente na proposta e na documentação.
- 12.3 Toda a documentação fará parte dos autos e **não será devolvida a licitante**, ainda que se trate de originais.
- 12.4 **Na contagem dos prazos estabelecidos nesta Chamanda de Oportunidade, excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. Os prazos estabelecidos neste edital para a fase externa se iniciam e se vencem somente em dias úteis de expediente da ETICE.**
- 12.5 Os representantes legais das Pré-Qualificadas são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

- 12.6 O desatendimento de exigências meramente formais, não essenciais, não implicará no afastamento da Pré-Qualificada, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.
- 12.7 A Comissão de Avaliação poderá sanar erros formais que **NÃO** acarretem prejuízos para o objeto da Chamada de Oportunidade, à Administração e às Pré-Qualificadas, dentre estes, os decorrentes de operações aritméticas.
- 12.8 Desde já fica estabelecido que caso a Pré-Qualificada **NÃO APRESENTE PROPOSTA** para a presente Chamada de Oportunidade, já está renunciando, assim, expressamente ao direito de recurso e respectiva contrarrazões, concordando com o curso desta Chamada de Oportunidade de Serviços de Nuvem Pública, aderente ao Edital de Pré-Qualificação Permanente de Serviços em Nuvem Nº 001/ 2019 – ETICE
- 12.9 Os casos omissos serão resolvidos pela Comissão de Avaliação, nos termos da legislação pertinente.
- 12.10 As normas que disciplinam esta Chamada de Oportunidade serão sempre interpretadas em favor da ampliação da disputa.
- 12.11 Os documentos referentes aos orçamentos, bem como o valor estimado da contratação, possuem caráter sigiloso e serão disponibilizados exclusivamente aos órgãos de controle interno e externo.
- 12.12 As Pré-Qualificadas deverão atender ao disposto no Código de Conduta, Ética e Integridade da ETICE, o qual encontra-se disponível no nosso sítio eletrônico para download.
- 12.13 O foro designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da **Comarca de Fortaleza**, Capital do Estado do Ceará.

Fortaleza,

36 de dezembro

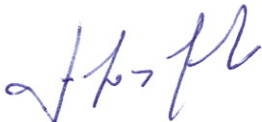
de 2021.

Elaborado por:



Marcos Antônio Marinho Russo
Diretor de Tecnologia da Informação e Inovação

Aprovo:



José Lassance de Castro
Presidente da ETICE

ROL DE ANEXOS:

ANEXO A - ESPECIFICAÇÃO TÉCNICA DA SOLUÇÕES DE PROTEÇÃO DE DADOS E FIREWALL

ANEXO B - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE GERENCIAMENTO, ORQUESTRAÇÃO DA NUVEM, SUSTENTAÇÃO EMERGENCIAL, ADMINISTRAÇÃO DOS PROJETOS

ANEXO C - CATALOGO DE SERVIÇOS DE NUVEM;

ANEXO D - LISTA DE PERFIS TÉCNICOS;

ANEXO E – MODELO DE PROPOSTA;

ANEXO F – TERMO DE RENÚNCIA.

ANEXO A

ESPECIFICAÇÃO TÉCNICA DA SOLUÇÕES DE PROTEÇÃO DE DADOS E FIREWALL

1. Solução de proteção de dados

- 1.1 Deverão ser fornecidas licenças para todas as funcionalidades solicitadas na modalidade por Licenciamento do Software
- 1.2 Deverão ser fornecidas licenças por TB, conforme quantidade definidas na tabela da proposta, encontrados na origem para ambientes virtuais, , incluindo todas as funcionalidades solicitadas neste termo, com suporte para backup, restore e tecnologia de deduplicação de dados, onde o licenciamento deve possuir capacidade ilimitada de retenções, cópias dos dados protegidos, replicações para outros ambientes para fins de recuperação de desastres;
- 1.3 A solução de Proteção de Dados a ser ofertada deve atender integralmente os requisitos especificados neste Termo, devendo ser fornecida com todas as licenças que forem necessárias para entrega funcional da solução;
- 1.4 Deverá possuir uma arquitetura em múltiplas camadas permitindo desempenho e escalabilidade horizontal:
- 1.5 Camada de gerência;
- 1.6 Camada do serviço de mídia/unidade de disco de retenção dos dados;
- 1.7 Camada de clientes/agentes multiplataforma de backups;
- 1.8 Deve possuir catálogo ou banco de dados centralizado contendo as informações sobre todos os dados e mídias onde os backups foram armazenados, esse banco de dados ou catálogo deve ser próprio e fornecido em conjunto com o produto;
- 1.9 Deve possuir mecanismo de verificação e checagem de consistência da base de dados no intuito de garantir a integridade dos dados;
- 1.10 Possuir mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda do mesmo, sem a necessidade de recatálogo as imagens de backup;
- 1.11 Deve suportar servidor de gerência e catálogo nas seguintes plataformas: Unix, Linux e Windows. Para evitar aumento de complexidade de gestão, não serão aceitos catálogos instalados em máquinas virtuais em plataformas (sistemas operacionais) diferentes da utilizada no servidor de gerência;
- 1.12 Deverá permitir a configuração de servidores de gerência de catálogo em cluster para promover alta-disponibilidade dos serviços de gerenciamento. A implementação do cluster deverá ser possível pelo menos para as plataformas: AIX, HP-UX, Red Hat Enterprise Linux, Oracle Linux, Solaris (SPARC e x86), Suse Enterprise Linux e Windows;
- 1.13 Deve suportar servidores movimentadores de dados nas seguintes plataformas: Unix, Linux e Windows.

- 1.14 Os servidores movimentadores de dados devem suportar balanceamento de carga para distribuir a carga de entre os mesmos de forma automática
- 1.15 Os servidores movimentadores de dados devem suportar configuração de recurso automático de failover, ou seja, permitir a configuração de mais de um servidor movimentador de dados em uma política de proteção, de forma que a indisponibilidade de um servidor seja suprida por outro servidor movimentador de dados disponível de forma automática. Esta funcionalidade deverá ser nativa do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros;
- 1.16 Deve permitir o backup e restore de arquivos abertos, garantindo a integridade do backup;
- 1.17 Possuir a capacidade de escrever múltiplos fluxos de dados provenientes de servidores distintos (multiplexação), divididos em blocos de tamanhos constantes em um único dispositivo físico de gravação;
- 1.18 Possuir a capacidade de dividir o fluxo de dados proveniente de um servidor em vários dispositivos de gravação (multiple streams);
- 1.19 Possuir a capacidade de reiniciar backups e restores a partir do ponto de falha, após a ocorrência da mesma;
- 1.20 Deve possuir mecanismo de atualização de clientes e agentes de backup de forma remota, através da interface de gerenciamento, permitindo a atualização de múltiplos clientes de backup simultaneamente;
- 1.21 Para facilitar o processo de verificação de pré-requisitos e compatibilidade, o fabricante deve possuir mecanismo público de geração de lista de checagem que, através da informação do pacote a ser instalado, do sistema operacional alvo da instalação, gere uma lista que contenha:
- 1.22 Patches do Sistema Operacional e de dispositivos de hardware que porventura necessitem estar instalados;
- 1.23 Componentes do produto suportados para instalação ou uso no Sistema Operacional em questão;
- 1.24 Requerimentos de Hardware para instalação do produto no Sistema Operacional em questão;
- 1.25 Componentes de Hardware compatíveis;
- 1.26 Compatibilidade com aplicações, bancos de dados e sistemas de arquivos (File System);
- 1.27 Possíveis correções e atualizações adicionais disponíveis para o funcionamento do produto no Sistema Operacional alvo.
- 1.28 Possuir a capacidade de realizar download e instalação de atualizações, de forma automática, no servidor de backup e clientes;
- 1.29 Possuir ambiente de gerenciamento de backup e restore via interface gráfica e linha de comando;
- 1.30 Possuir função de agendamento do backup através de calendário;
- 1.31 Possuir interface gráfica para gerenciamento, monitoramento e criação de políticas de backup e restore;

- 1.32 Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup;
- 1.33 Permitir a programação de tarefas de backup automatizadas em que sejam definidos prazos de retenção dos arquivos;
- 1.34 Possuir função para definição de prioridades de execução de Jobs de backup;
- 1.35 Deve permitir o agendamento de jobs de backup, sem utilização de utilitários de agendamento dos hosts;
- 1.36 Deve permitir a programação de jobs de backup automatizadas em que sejam definidos prazos de retenção das imagens;
- 1.37 Possuir a função de Backup sintético que permite a criação de uma única imagem de backup a partir de um backup full e qualquer quantidade de backups incrementais. O restore será efetuado da nova imagem full sintética;
- 1.38 Possuir políticas de ciclo de vida nativas, gerenciar camadas de armazenamento e transferir automaticamente os dados de backup entre camadas através do seu ciclo de vida;
- 1.39 Permitir a realização do backup completo de servidor para recuperação de desastres;
- 1.40 Permitir restaurar o backup de recuperação de desastres para hardware diferente do original - para ambiente Windows;
- 1.41 Permitir o controle da banda de tráfego de rede durante a execução do backup e/ou do restore;
- 1.42 Suportar a proteção dos dados de aplicações de big data Hadoop e AHV (Nutanix Acropolis Hypervisor)
- 1.43 Ser capaz de recuperar dados para servidores diferentes do equipamento de origem;
- 1.44 Permitir integração do controle de acesso com sistemas de diretório NIS, NIS+ e Active Directory;
- 1.45 Permitir a replicação de imagens de um servidor de gerência para outro ambiente, possibilitando a inserção das informações de catálogo da imagem de origem para o catálogo do destino, de forma automática e sem a necessidade de licenciamento adicional.
- 1.46 Possuir Interface única para gerenciamento de todos os servidores independente do S.O que hospeda esse serviço (Windows, Linux); ou ao menos com a separação entre estrutura de backup da Central de Serviços e estrutura de backup das Unidades remotas.
- 1.47 Deve implementar monitoramento e administração remotos da solução de backup a partir de qualquer servidor ou estação de trabalho Windows;
- 1.48 A Solução de Backup deverá permitir operações de Backup e Restore através de rede local (LAN_based e Storage Area Network (SAN_based ou LAN_free);
- 1.49 A Solução de Backup deverá, a partir de uma única interface, gerenciar operações de Backup e Restore de diferentes sistemas operacionais (clientes); bem como operações de recuperação bare metal.

- 1.50 Deve permitir a criação de imagens de servidores físicos, Linux e Windows, para recuperação de desastres (funcionalidade conhecida como bare metal restore de forma nativa, i.e., sem a utilização de software de terceiros;
- 1.51 Para servidores Windows, deve ser possível a recuperação das imagens de recuperação de desastres mesmo em um hardware diferente do original ou em ambiente virtual.
- 1.52 A funcionalidade de baremetal especificada anteriormente deve suportar em um único servidor de gerência ou servidor de mídia várias versões de Windows – Windows 2008, 2008 R2, 2012 e 2012R2).
- 1.53 Deve permitir a verificação da integridade dos dados armazenados através de algoritmos de checksum e/ou autocorreção;
- 1.54 Deve permitir escolher se a criptografia será realizada no agente, com o tráfego de dados via rede já criptografado ou no servidor de backup;
- 1.55 Deve possuir capacidade nativa de efetuar criptografia dos backups em no mínimo 256 bits nos Clientes de Backup e em dispositivos de mídia que suportem criptografia;
- 1.56 Deve possuir a capacidade de gerenciar software de snapshot de storages de outros fabricantes, tais como Dell EMC, Netapp, HPE, Nutanix e Pure com o intuito de automatizar o processo de agendamento de cópias “snapshot” e montagem no servidor de backup “off-host”;
- 1.57 Deverá possuir integração para gerência de Snapshots;
- 1.58 Deverá permitir a criação e gerenciamento de Snapshots através da ferramenta de administração da Solução de Backup;
- 1.59 Possibilitar o registro dos Snapshots na base relacional de catálogos da Solução de Backup de forma a possibilitar a realização de buscas;
- 1.60 Controlar o período pelo qual os Snapshots serão válidos, realizando a expiração automática de um Snapshot assim que o período de retenção configurado seja atingido.
- 1.61 Deve possibilitar enviar notificações, quando configurado, dos eventos por e-mail;
- 1.62 Possuir mecanismo de auditoria, permitindo a emissão de relatórios onde constem, no mínimo, as seguintes informações:
- 1.63 Data e hora da operação, Usuário que realizou a operação, Ação realizada (em caso de modificação de configurações, informar qual a configuração anterior e a modificação realizada).
- 1.64 Auditoria e controle de acesso devem ser funcionais para operações realizadas via interface gráfica e linha de comando.
- 1.65 Deve prover monitoramento via interface gráfica e em tempo real dos Jobs sendo executados, incluindo visão de nível hierárquico dos jobs.
- 1.66 Deve permitir encadear Jobs para que um só comece após outro ter terminado;
- 1.67 Deve suportar armazenamento nos cloud storages: Amazon S3, Microsoft Azure e Google Cloud Storage.
- 1.68 Permitir o controle da banda de tráfego de rede durante a execução do backup para nuvem

- 1.69 Deve suportar o backup e o restore de diferentes sistemas operacionais tais como:
 - 1.69.1 Windows (7/8/10/2012 R2/2016/2019);
 - 1.69.2 Oracle Linux (6 e 7);
 - 1.69.3 Red Hat Enterprise Linux (6 e 7);
 - 1.69.4 Suse Enterprise Server (11 e 12);
 - 1.69.5 CentOS (6 e 7);
 - 1.69.6 Debian GNU (7, 8 e 9);
 - 1.69.7 Oracle Solaris (10 e 11);
 - 1.69.8 AIX (6.1, 7.1 e 7.2);
 - 1.69.9 Ubuntu (16, 17 e 18)
- 1.70 Suportar a tecnologia de virtualização da Vmware.
- 1.71 Deve possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais;
- 1.72 Deve possuir capacidade de realizar backup de máquinas virtuais em estado online ou offline;
- 1.73 Deve suportar os seguintes bancos de dados, utilizando agente específico:
 - 1.73.1 Microsoft SQL Server versões 2012, 2014, 2016, 2017;
 - 1.73.2 Oracle/Oracle RAC versões 11g, 12c e 18c.
 - 1.73.3 Microsoft Exchange 2010, 2013 e 2016;
 - 1.73.4 Microsoft Sharepoint 2010, 2013 e 2016;
 - 1.73.5 MySQL 5 e 8;
 - 1.73.6 PostgreSQL 9, 10 e 11;
 - 1.73.7 MariaDB 5 e 10;
 - 1.73.8 Microsoft Active Directory
- 1.74 Deve suportar backup do Oracle Database, também na arquitetura Oracle RAC, através da integração com RMAN;
- 1.75 Deve manter a sincronia entre os catálogos de backups do Oracle RMAN e da solução ofertada;
- 1.76 Deve possuir funcionalidade para descoberta automática de instancias Oracle através de consultas periódicas aos clientes de bancos de dados;
- 1.77 A funcionalidade de descoberta automática de instancias deve ser capaz de gerar os scripts RMAN no momento de execução do backup;
- 1.78 Deve suportar Apache Hadoop e Apache HBase;
- 1.79 Deve suportar DAG (DataBase Availability Groups) do MS Exchange;
- 1.80 Deve suportar backup do Microsoft Active Directory, com possibilidade de restore granular, ou seja, restauração de todo um diretório, de objetos selecionados e até de atributos individuais;
- 1.81 Deve suportar backup completo do Sharepoint, com possibilidade de recuperação de uma ou mais databases, documentos individuais, sites, subsites, listas e itens/documentos individuais;
- 1.82 Desduplicação por Software
- 1.83 Deve possuir capacidade de realizar desduplicação de dados na camada no cliente, servidor de backup e appliances de desduplicação. A solução deve permitir a desduplicação de qualquer capacidade (de acordo com o volume

- identificado e licenciado) e em qualquer forma de desduplicação (cliente, servidor de backup e appliances);
- 1.84 Deve suportar desduplicação de blocos na origem (client-side), de forma que o cliente envie apenas novos blocos de dados criados e/ou modificados a partir do último backup full;
- 1.85 Deverá suportar o envio de dados desduplicados para a nuvem.
- 1.86 A solução de backup deve ser capaz de gerenciar a réplica do backup desduplicado entre appliances de desduplicação.
- 1.87 Deve possuir a capacidade de desduplicação global de dados no nível de segmentos ou blocos de dados repetidos, entre ambientes físicos e virtuais, mesmo em localidades remotas;
- 1.88 Deve possuir a capacidade de Replicação de Dados entre “pools” de desduplicação de maneira otimizada, enviando somente blocos únicos.
- 1.89 Deverá possibilitar a distribuição automática de carga entre os servidores que executarão o serviço de proteção de dados, ou seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de backup da solução. Em caso de falha de um dos servidores de backup, o cliente automaticamente irá encaminhar seus dados através de outro servidor de backup ativo. Esta funcionalidade deverá ser nativa do produto, não sendo admitidas soluções baseadas em softwares de cluster de terceiros;
- 1.90 As políticas de ciclo de vida da informação devem permitir a replicação das imagens de backup de forma otimizada, fazendo o uso da tecnologia de desduplicação de dados da solução no mesmo site ou entre sites distintos;
- 1.91 Deve fazer uso de tecnologia de replicação dos dados (não somente os dados protegidos – imagens de backup – mas também do catálogo do software de backup necessário para a recuperação do dado) do site principal para o site de desastre, de forma que em um evento de desastre, os sites sejam independentes no processo de recuperação.
- 1.92 Deve possuir tecnologia de desduplicação de dados inline por padrão
- 1.93 Relatórios e Gerenciamento
- 1.94 Relatórios Operacionais
- 1.95 Deve prover relatórios gerenciais de backup com no mínimo as seguintes informações:
- 1.96 Backups com sucesso;
- 1.97 Backups com falha;
- 1.98 Volume de backup realizado;
- 1.99 Restores com sucesso;
- 1.100 Restores com falha;
- 1.101 Volume de restore realizado;
- 1.102 Clientes de backup configurados;
- 1.103 Ocupação no destino de backup;
- 1.104 Licenciamento e capacidade;
- 1.105 Interface Web De Gerenciamento

- 1.106 Possuir interface web para gerenciamento, monitoramento, emissão de alertas, emissão de relatórios sobre operações de backup e restore e emissão de relatórios, com as seguintes características:
- 1.107 Relatórios sobre capacidade e tendência de crescimento do ambiente;
- 1.108 Se houver múltiplos ambientes de backup, com independência operacional e localizados em diferentes Data Centers, deve possuir nativamente uma única interface web deve ser capaz de monitorar e agregar informações de diversos Servidores da Camada de Gerenciamento para emissão dos relatórios;
- 1.109 Relatórios para verificar o nível de serviço, ou seja, visualização de que aplicações estão com políticas de backup ativadas e executadas periodicamente;
- 1.110 Deve permitir exportar relatórios;
- 1.111 Base de dados de relatórios para suportar armazenamento de dados históricos superior a 30 dias;

2. Solução de Firewall para Nuvem

2.1 CARACTERÍSTICAS GERAIS

- 2.2 O licenciamento deverá ser feito pelo número de cores virtuais;
- 2.3 Deve ser compatível com, pelo menos, os seguintes hypervisors: VMware ESXi, Microsoft Hyper-V e KVM;
- 2.4 A solução deverá permitir expansão através de adição de novas licenças, de forma que suporte à criação de "pools" de gateways virtuais;
- 2.5 A solução para ambientes virtualizados deve suportar os seguintes SDN de mercado para integração: OpenStack, Cisco ACI, VMware NSX, e ESXi.

2.6 FUNCIONALIDADES GENÉRICAS DE FIREWALL

- 2.7 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
- 2.8 Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server e Jumbo Frames;
- 2.9 DEVE SUPORTAR OS SEGUINTE TIPOS DE NAT:
- 2.10 Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;
- 2.11 Enviar logs para sistemas de monitoração externos, simultaneamente;
- 2.12 Prover mecanismo de prevenção a ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deverá se originar;
- 2.13 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 2.14 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 2.15 Suportar OSPF graceful restart;
- 2.16 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

- 2.17 FUNCIONALIDADES DE FILTRO DE CONTEÚDO WEB
- 2.18 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;
- 2.19 Controle de políticas por usuários, grupos de usuários, IPs e redes;
- 2.20 Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
- 2.21 Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- 2.22 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
- 2.23 Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
- 2.24 Reconhecer pelo menos 2.900 (duas mil e novecentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 2.25 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;
- 2.26 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
- 2.27 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;
- 2.28 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;
- 2.29 Atualizar a base de assinaturas de aplicações automaticamente;
- 2.30 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
- 2.31 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 2.32 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
- 2.33 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do banco;
- 2.34 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 2.35 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

- 2.36 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 2.37 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
- 2.38 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local;
- 2.39 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
- 2.40 Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;
- 2.41 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs;
- 2.42 Suportar a criação de categorias de URLs customizadas;
- 2.43 Suportar a exclusão de URLs do bloqueio, por categoria;
- 2.44 Permitir a customização de página de bloqueio;
- 2.45 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;
- 2.46 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários;
- 2.47 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);
- 2.48 **FUNCIONALIDADES DE PREVENÇÃO DE AVEAÇAS**
- 2.49 Os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento;
- 2.50 Deve incluir assinaturas de prevenção de intrusão (IPS) e suporte ao bloqueio de arquivos maliciosos (Antivírus e Anti-Malware);
- 2.51 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 2.52 Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 2.53 Deverá possuir os seguintes mecanismos de inspeção de IPS:
- 2.54 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
- 2.55 Detectar e bloquear a origem de portscans;

- 2.56 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
- 2.57 Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 2.58 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
- 2.59 Suportar bloqueio de arquivos por tipo;
- 2.60 Identificar e bloquear comunicação com botnets;
- 2.61 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
 - 2.62 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
 - 2.63 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware;
 - 2.64 Os eventos devem identificar o país de onde partiu a ameaça;
 - 2.65 Suportar rastreamento de vírus em arquivos pdf;
 - 2.66 Deve suportar a inspeção em arquivos comprimidos (zip, gzip, etc.);
 - 2.67 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
 - 2.68 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
 - 2.69 Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia, não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;
- 2.70 **PREVENÇÃO DE AMEAÇAS AVANÇADAS**
- 2.71 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real e inspeção com prevenção de tráfego de saída de callbacks (comunicação do malware com o servidor de comando e controle);
- 2.72 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL's conhecidas;
- 2.73 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP (32 bits), Windows 7 (32 e 64 bits), Windows 8, Windows 8.1 e Windows 10 (64 bits), assim como Office 2003, 2010 e 2013;
- 2.74 Implementar gerenciamento SNMP v2 e v3;
- 2.75 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
- 2.76 Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: cab, csv, doc, docx, docm, dot, dotm, dotx, exe, hwp, jar, pdf, pif, ppam, pps, ppsm, ppsx, potx, potm, ppt, pptm, pptx, rar, rtf, seven-z, sldm, sldx, swf, tar, tgz, xlam, xls, xlsx, xlt, xltx, xlsx, xlsm, xltm, xll, xlsb, zip;

- 2.77 Prover informações para que a solução de relatórios possa apresentar via interface gráfica as seguintes informações:
- 2.78 Sumário executivo;
- 2.79 Relatório de máquinas infectadas;
- 2.80 Atividades do malware durante a execução de arquivo, nos ambientes controlados em todas as versões de sistemas operacionais requisitados neste projeto;
- 2.81 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
- 2.82 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
- 2.83 Número de arquivos emulados;
- 2.84 A solução de possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:
- 2.85 Arquivos scaneados;
- 2.86 Arquivos maliciosos;
- 2.87 **CONTROLE DE QUALIDADE DE SERVIÇO**
- 2.88 Suportar a criação de políticas de QoS por:
- 2.89 Endereço de origem, endereço de destino e por porta;
- 2.90 O QoS deve possibilitar a definição de classes por:
- 2.91 Banda garantida, banda máxima e fila de prioridade;
- 2.92 Disponibilizar estatísticas RealTime para classes de QoS;
- 2.93 **FUNCIONALIDADES DE VPN**
- 2.94 Suportar VPN Site-to-Site e Client-To-Site;
- 2.95 Suportar IPSec VPN;
- 2.96 Suportar SSL VPN;
- 2.97 A VPN IPSEc deve suportar:
- 2.98 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e autenticação via certificado IKE PKI;
- 2.99 A VPN SSL DEVE SUPORTAR:
- 2.100 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- 2.101 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 2.102 Atribuição de endereço IP nos clientes remotos de VPN;
- 2.103 Atribuição de DNS nos clientes remotos de VPN;
- 2.104 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
- 2.105 Suportar autenticação via AD/LDAP, certificado digital e base de usuários local;
- 2.106 Suportar leitura e verificação de CRL (certificate revocation list);
- 2.107 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e MacOS X;

ANEXO B

CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE GERENCIAMENTO, ORQUESTRAÇÃO DA NUVEM, SUSTENTAÇÃO EMERGENCIAL, ADMINISTRAÇÃO DOS PROJETOS

1. DA COMPLEXIDADE DO SERVIÇO

1.1 A adoção do valor de referência único facilita à contabilização dos serviços, todavia, demanda a definição dos parâmetros relativos a ponderação aplicável ao dimensionamento do serviço; nesse sentido, para efeito de cada projeto a ser contratado, serão adotados os seguintes pesos de complexidade:

Complexidade	Serviços	Peso Complexidade
Baixa	Monitoramento de chamados de terceiros. Atendimento aos usuários na modalidade emergencial. Assistência técnica remota (plantão). Atividades de apoio à: monitoramento de ações, acompanhamento de atividades, registros em sistemas básicos, formatação de artefatos básicos de projetos de sistemas, prototipação e atividades similares.	1,00
Intermediária	Assistência Técnica Presencial. Análise e levantamento de processos. Criação e implantação da base de conhecimento na solução de gerenciamento de serviços e atualização dos scripts de atendimento. Operação de sistemas complexos, apoiar na criação de artefatos de projetos, especificação casos de uso, regras de negócio, elaboração de diagramas de processos e estratégia, atendimento a demanda de média complexidade de clientes internos, mapeamento de processos e atividades similares.	1,05
Alta	Automação de processos na solução de gerenciamento de serviços. Desenvolvimento de painel de controle (<i>dashboard</i>), portfólio e catálogo de serviços. Desenvolvimento de novos relatórios. Implantação de novos processos, apoio na criação e desenvolvimento	1,10

	de projetos, estudos de viabilidade de projetos, criação de novos processos, desenvolvimento de novos sistemas, aperfeiçoamento de processos de gestão do cliente final ou Etice, apoio na implantação de novos sistemas no cliente final ou Etice, e atividades similares.	
Especialista	Customização na solução de gerenciamento de serviços. Execução de demanda eventual ou projeto não contemplado dos demais itens em razão de sua necessidade pontual de execução que requeiram conhecimento técnico em áreas correlatas sejam infraestrutura, sistemas, segurança da informação ou atividades similares.	1,15

Tabela B.1 - Definições de complexidade do serviço

1. DO CATÁLOGO DE SERVIÇOS

- 2.1 Conforme o ITIL, o Catálogo de serviço é um conjunto de informações sobre os serviços de TIC disponíveis para uso, trata-se de um conteúdo dinâmico, que requer revisão e alterações periódicas para que esteja adequado a realidade da TI, demandando assim um processo específico de gerenciamento, para que possa ser atual e aderente.
- 2.2 No contexto da presente especificação técnica, **buscou-se a elaboração de um catálogo que permitisse atender uma vasta gama de necessidades relativas a serviços em nuvem**, todavia, conforme as melhores práticas de gerenciamento de serviços e frameworks de mercado a exemplo do ITIL e COBIT o catálogo de serviços por tratar-se de um conteúdo dinâmico, necessita de revisões e adequações que venham a ser necessárias com vistas a assegurar sua aderência ao negócio. Assim com vistas a assegurar a aplicação das boas práticas de forma a suportar adequadamente as necessidades de negócio o catálogo de serviços que integra o presente instrumento estará sujeito a melhorias para a realização do objeto ajustado a realidade da Etice e dos seus clientes finais.
- 2.3 Em função da evolução da maturidade da Etice e em função da dinâmica dos processos, a versão inicial do catálogo de **serviços poderá sofrer revisões** com vistas a se adequar a realidade da Etice e de seus clientes finais na ocasião, através de projetos específicos para revisão do catálogo de serviços.
- 2.4 A versão inicial do Catálogo de Serviços - (ANEXO C) elenca os tipos de solicitações contempladas pelo objeto do serviço, fornecendo referência a parâmetros que definem a ponderação do serviço.

3. DAS CONDIÇÕES DE EXECUÇÃO

- 3.1 O objeto desta especificação técnica tem por escopo **serviços de natureza contínua, prestados sob demanda**, para operacionalização de processos descritos no catálogo de serviços, assim como serviços pontuais, prestados sob demanda para a execução de projetos, que venham a ser necessários a efetivação dos objetivos estratégicos da Etice e seus cliente finais no que dependam da tecnologia da informação e comunicação usando ambiente de nuvens.
- 3.2 A Etice poderá a seu critério utilizar as USTs contratadas para a execução de serviços continuados (processos) ou pontuais (projetos) sem ônus ao objeto contratual, considerando especificações do catálogo de serviços.

5. DA SOLICITAÇÃO DE SERVIÇOS

- 5.1. Mensalmente ou em caso de necessidade serão abertas ordens de serviço, com os Serviços Técnicos devidamente identificados e associados a uma estimativa (UST) relacionadas aos serviços a serem executados.
- 5.2. A partir da abertura da OS, todas as atividades necessárias para a execução dos serviços deverão estar relacionadas às demandas devidamente registradas em ferramenta de Gestão de Demandas. Quando não houver disponibilidade desta ferramenta, poderá ser realizada por qualquer outra compatível.
- 5.3. Para o encerramento de uma demanda é necessário o registro das atividades que evidenciam o seu atendimento.
- 5.4. O cálculo do número de USTs relativas aos serviços solicitados, será realizado por ocasião da emissão da ordem de serviços (OS) que poderá contemplar a execução de um ou mais serviço. Esse agrupamento só deverá ser aplicado para serviços com durações semelhantes, para não ocasionar retardo no encerramento da OS. O referido cálculo deverá ser feito para cada serviço solicitado na OS conforme a seguinte fórmula:

$$\text{UST} = (\text{Esforço} \times \text{complexidade})$$

onde:

UST: corresponde ao quantitativo de unidades de serviços técnicos estimados para a realização do serviço.

Esforço: Somatório da estimativa de todos esforços decorrentes da alocação temporal de um ou mais recursos necessários ao serviço, considerados os pesos aplicados a cada recurso. Ou seja, **Esforço = Fator * Número de horas alocadas**.

Complexidade: peso quanto ao tipo predominante de atividades inerentes a sua realização do serviço.

- 5.5. Para aplicação da fórmula da UST ajustada por serviço, deve-se considerar que:
- 5.5.1. O dimensionamento do esforço para o serviço demandará estudo para definição de estimativas da alocação recursos necessários ao serviço, considerando quantitativos e a alocação temporal dos recursos para atendimento demanda.
- 5.5.2 A CONTRATADA poderá adotar o fator médio de 1,368 do ANEXO D para dimensionar o esforço;

5.5.3. Caso opte por não usar o fator médio a CONTRATADA deverá dimensionar o esforço adotando os pesos definidos no ANEXO D – LISTA DE PERFIS TÉCNICOS dos recursos;

6. DO CANCELAMENTO DOS SERVIÇOS

6.1. Nos casos em que a demanda for cancelada por solicitação do cliente final ou da Etice, o trabalho já executado deverá ser medido, avaliado e pago.

6.2. Quando do cancelamento do serviço, a CONTRATADA deverá entregar os produtos do serviço executado, imediatamente, mesmo que inacabados.

6.3. O pagamento dos serviços cancelados está vinculado à entrega dos produtos parciais elaborados pela CONTRATADA até o momento do cancelamento.

21
11

ETIC

Pág

ANEXO C

CATALOGO DE SERVIÇOS DE NUVEM

O catálogo de serviços apresentado na tabela abaixo lista as complexidades esperadas para cada serviço a ser executado.

Este catálogo pode ser alterado pontualmente na medição de serviços no caso de ser detectado pela Etice e aprovado pela SSPDS que o serviço apresenta para uma determinada atividade uma complexidade diferente da listada.

Este catálogo pode ser alterado permanentemente no caso de ser detectado pela Etice e aprovado pelo SSPDS que o serviço apresenta para a maioria das atividades relacionadas a ele uma complexidade diferente da listada.

SERVIÇO	COMPLEXIDADE
Avaliação e descoberta de portfólio de aplicações e suas interdependências para construção de plano para migração.	Intermediário
Avaliação de infraestrutura existente para dimensionamento de infraestrutura necessária em ambiente de nuvem	Intermediário
Migração de cargas de trabalho Microsoft Windows Server, SQL e .NET	Intermediário
Migração de bases de dados on-premises para nuvem, com ou sem atualização de versão, para: outros motores suportados; bases de dados para propósitos específicos (NoSQL).	Alta
Migração de containers on-premises para soluções de orquestração e repositório de containers gerenciados.	Alta
Migração de cargas de trabalho, elegíveis, de máquinas virtuais para containers	Alta
Migração de cargas de trabalho, elegíveis, máquinas virtuais ou containers para modelo sem servidor	Alta
Migração de cargas de trabalho em máquinas virtuais para serviços gerenciados elegíveis	Alta
Implementação de mecanismo de alta disponibilidade, escalabilidade horizontal automatizada, monitoramento,	Alta

verificações de saúde e balanceamento de carga	
Construção de data warehouse a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Implementação de rede de entrega de conteúdo (CDN) para conteúdo (site) estáticos	Intermediário
Criação/configuração de topologia de redes interconectadas com isolamento, firewall, ACL's (Access Control Lists) e auditoria	Intermediário
Implementação e configuração de conectividade do ambiente on-premises com ambiente em nuvem	Intermediário
Configuração de serviço de DNS, público ou privado, e integração com serviço de DNS on-premises	Intermediário
Implementação de modelo de categorização de custos com base em rótulos, orçamentos e alarmes de consumo mensal	Baixa
Implementação de controles para filtro de requisições Web classificadas como nocivas	Intermediário
Configuração de cofre de senhas para armazenamento de credenciais, chaves e outros dados sensíveis	Intermediário
Automação do provisionamento e gerência de configuração de serviços e recursos de nuvem com modelo de infraestrutura como código e auto-serviço	Alta
Implementação de solução para gerenciamento e automação de backup de dados nos serviços de nuvem ou ambiente on-premises	Intermediário
Implementação de solução para backup de dados de longa retenção com políticas de ciclo de vida	Intermediário
Fornecimento de sistemas no modelo Software as Service	Intermediário
Implementação de processos de transferência de grandes volumes de dados para nuvem, incluindo processo de backup e restauração em novo ambiente	Intermediário
Desenho e implantação de arquitetura para continuidade de negócios e recuperação de desastres em ambiente de nuvem de acordo com requisitos de RTO (Recovery Time Objective) e RPO	Especialista

(Recovery Point Objective)	
Apresentação de workshops/transferência de conhecimento para detalhamento de entregáveis	Baixa
Configuração de estrutura de contas em conformidade com melhores práticas de segurança	Intermediário
Desenvolvimento, monitoramento e sustentação de software	Intermediário
Avaliação de ambiente em nuvem sobre perspectiva de segurança, desempenho, confiabilidade, custos e eficiência operacional e aplicação de correções apropriadas	Alta
Migração fim-a-fim de máquinas virtuais incluindo os processos de conversão, importação, configuração e testes do ambiente migrado.	Alta
Implementação de ambiente para virtualização de desktops, incluindo configuração de redes, autenticação, políticas de gerenciamento e imagens personalizadas com configurações e aplicativos	Alta
Gerenciamento dos provedores de serviço, orquestração, bilhetagem, implementação de mecanismos de controle, otimização de custos, sustentação e operação de ambiente de Nuvem com execução de tarefas do dia-a-dia: monitoramento, aplicações de patches, backup, atendimento de requisições de tarefas e mudanças.	Baixa

ANEXO D - LISTA DE PERFIS TÉCNICOS

1. A tabela a seguir estabelece relação entre os perfis técnicos dos recursos a serem alocados na execução dos serviços, sejam profissionais ou materiais, com o peso adotado do para efeito de cálculo do esforço considerado no dimensionamento de USTs do serviço.

Item	Perfil Técnico	Requisitos Técnicos Mínimos Obrigatórios de Enquadramento	Peso
1	Auxiliar Técnico I	<p>Do Auxiliar Técnico de TIC de Nível I</p> <p>Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência comprovada e no mínimo 01 (um) ano em atividades e funções correlatas ao serviço.</p> <p>Do Auxiliar Técnico de Processo de Negócio de Nível I</p> <p>Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto da atividade, com experiência comprovada e no mínimo 01 (um) ano em atividades e funções correlatas ao serviço.</p>	0,25
2	Auxiliar Técnico II	<p>Do Auxiliar Técnico de TIC de Nível II</p> <p>Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência comprovada e no mínimo 02 (dois) anos em atividades e funções correlatas ao serviço.</p> <p>Do Auxiliar Técnico de Processo de Negócio Nível II</p> <p>Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto da atividade, com experiência comprovada e no mínimo 02 (dois) anos em atividades e funções correlatas ao serviço.</p>	0,50
3	Técnico I	<p>Do Técnico de TIC de Nível I</p> <p>Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 03 (três) anos em atividades e funções correlatas ao serviço.</p> <p>Do Técnico de Processo de Negócio Nível I</p>	1

		Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto da atividade, com experiência mínima de, 03 (três) anos em atividades e funções correlatas ao serviço.	
4	Técnico II	<p style="text-align: center;">Do Técnico de TIC de Nível II</p> <p>Enquadram-se profissionais com formação de nível superior em andamento com, pelo menos, 50% (cinquenta por cento) do curso concluído em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço com experiência comprovada de no mínimo 03 (três) anos em atividades e funções correlatas ao serviço.</p> <p style="text-align: center;">Ou</p> <p>Alternativamente, profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 05 (cinco) anos em atividades e funções correlatas ao serviço.</p> <p style="text-align: center;">Do Técnico de Processo de Negócio Nível II</p> <p>Enquadram-se profissionais com formação de nível superior em andamento com, pelo menos, 50% (cinquenta por cento) do curso concluído em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de no mínimo 03 (três) anos em atividades e funções correlatas ao serviço.</p> <p style="text-align: center;">Ou</p> <p>Alternativamente, profissionais com formação de nível médio em qualquer em área compatível com o processo de negócio objeto da atividade, com experiência comprovada mínima de 05 (cinco) anos em atividades e funções correlatas ao serviço.</p>	1,5
5	Analista I	<p style="text-align: center;">Do Analista de TIC de Nível I</p> <p>Enquadram-se os profissionais com formação de nível superior em área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 05 (cinco) anos em atividades e funções correlatas ao serviço,</p> <p style="text-align: center;">Do Analista de Processo de Negócio Nível I</p> <p>Enquadram-se profissionais com formação de nível</p>	2,0

		superior compatível com o processo de negócio objeto da atividade, com experiência mínima de 05 (cinco) anos em atividades e funções correlatas ao processo objeto da atividade.	
6	Analista II	<p style="text-align: center;">Do Analista de TIC de Nível II</p> <p>Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Lato Sensu) concluída ou em andamento em área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 06 (seis) anos em atividades e funções correlatas ao serviço;</p> <p style="text-align: center;">Ou,</p> <p>Alternativamente, formação de nível superior compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 08 (oito) anos em atividades e funções correlatas ao serviço.</p> <p style="text-align: center;">Do Analista de Processo de Negócio Nível II</p> <p>Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Lato Sensu) concluída ou em andamento em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de no mínimo 06 (seis) anos em atividades e funções correlatas ao processo objeto da atividade.</p> <p style="text-align: center;">Ou,</p> <p>Alternativamente, formação de nível superior compatível com o processo de negócio objeto da atividade, com experiência mínima de 08 (oito) anos em atividades e funções correlatas ao processo objeto da atividade.</p>	2,50
7	Especialista I	<p style="text-align: center;">Do Especialista de TIC de Nível I</p> <p>Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Lato Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 07 (sete) anos em atividades e funções correlatas ao serviço;</p> <p style="text-align: center;">Ou,</p> <p>Alternativamente, formação de nível superior compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço,</p>	3,00

		<p>certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao serviço.</p> <p>Do Especialista de Processo de Negócio Nível I</p> <p>Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Lato Sensu) em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de, no mínimo, 07 (sete) anos em atividades e funções correlatas ao processo objeto da atividade.</p> <p>Ou,</p> <p>Alternativamente, formação de nível superior compatível com o processo de negócio objeto da atividade, com certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao processo objeto da atividade.</p>	
8	Especialista II	<p>Do Especialista de TIC de nível II</p> <p>Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Stricto Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço e experiência comprovada de, no mínimo, 08 (oito) anos em atividades e funções correlatas ao serviço,</p> <p>Ou,</p> <p>Alternativamente, formação de nível superior e pós-graduação (no mínimo Lato Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao serviço.</p> <p>Do Especialista de Processo de Negócio nível II</p> <p>Enquadram-se os profissionais com formação de nível superior e pós-graduação (no mínimo Stricto Sensu) em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de, no mínimo, 08 (oito) anos em atividades e funções correlatas ao processo objeto da atividade;</p> <p>Ou,</p>	3,50

		Alternativamente, formação de nível superior e pós-graduação (no mínimo Lato Sensu) compatível com o processo de negócio objeto da atividade, com certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao processo objeto da atividade.	
--	--	---	--

3. Com vistas a favorecer o processo de precificação do serviço no que se refere a alocação de recursos necessários ao serviço, considerada a necessidade de execução contínua de dadas atividades, a aceitabilidade definida dos perfis por serviços relacionados no catálogo de serviços, e cenários atuais relativos aos serviços demandados, estima-se que para correta execução dos serviços, os recursos necessários serão alocados com base na seguinte distribuição de tempo:

Perfil Técnico	Alocação estimada
Auxiliar I	17%
Auxiliar II	17%
Técnico I	16%
Técnico II	16%
Analista I	16%
Analista II	8%
Especialista I	5%
Especialista II	5%

4. Considerando os serviços listados no catálogo, seus pesos e distribuições adote-se apenas como referência para precificação, o fator médio de 1,368 para conversão entre horas de alocação e UST conforme a seguinte fórmula: Número de horas alocadas = (Número de UST_mês/(1,368*COMPLEXIDADE)). Esse fator foi definido com consideração a média de todos os pesos aplicáveis aos serviços no catálogo, permitindo uma aproximação do quantitativo em horas, da alocação necessária de recursos para a execução dos serviços.
- 4.1 A CONTRATADA deverá propor um fator diferente do fator médio para aqueles casos em que a alocação real não está de acordo com a alocação estimada, o qual será avaliado pela CONTRATANTE.

ANEXO E – Modelo de Proposta

Tabela 1–Cessão de direito de Uso de Software para Nuvem

ITEM	DESCRIÇÃO	Unidade	QTD (a)	Valor Unitário Mensal (b)	Valor Anual (c = 12 x a x b)
1	Cessão de direito de uso de Software de Proteção de Dados para Nuvem	LICENÇA	100		
2	Cessão de direito de uso de Software de Firewall para Nuvem	LICENÇA	40		
3	Cessão de direito de uso de Software de Microsoft Server Data Center para Nuvem	LICENÇA	300		
4	Cessão de direito de uso de Software de VMware vSphere Enterprise Plus para Nuvem	LICENÇA	40		
5	Cessão de direito de uso de Software de VMware vRealize Cloud Universal Advanced para Nuvem	LICENÇA	40		
6	Cessão de direito de uso de Software de VMware vRealize Cloud Universal Enterprise para Nuvem	LICENÇA	40		
7	Cessão de direito de uso de Software de VMware NSX Data Center Advanced para Nuvem	LICENÇA	40		
8	Cessão de direito de uso de Software de Vmware VCenter para Nuvem	LICENÇA	5		
Soma (d)					

(t1)Valor Total em R\$ (igual a “d”)

- Tabela 2 –Serviços Diversos

ITEM	DESCRIÇÃO	Unidade	QTD Anual (a)	Valor Unitário (b)	Valor Anual (c = a x b)
9	Serviços de gerenciamento, orquestração da nuvem, sustentação, administração dos projetos.	UST	30.000		
Soma (d)					

(t2) Valor Total em R\$ (igual a “d”)

Valor Total da Proposta (t1+t2)

ANEXO F – Termo de Renúncia

<PAPEL TIMBRADO DA EMPRESA>

TERMO DE RENÚNCIA DE OFERECIMENTO DE PROPOSTA

À

Comissão Especial de Organização e Avaliação de Chamadas de Oportunidades de Serviços em Nuvem - Empresa de Tecnologia da Informação do Ceará – Etice

Referência: Chamada de Oportunidade nº 001/2021

Prezada Comissão,

Declaramos, na forma e sob as penas da Lei, que não ofereceremos proposta para a Chamada de Oportunidade nº 001/2021, publicada em 17 de fevereiro de 2021, renunciando, assim, expressamente ao direito de recurso e ao prazo respectivo e concordando com o curso desta Chamada de Oportunidade de Serviços de Nuvem Pública, aderente ao Edital de Pré-Qualificação Permanente de Serviços em Nuvem Nº 001/ 2019 – ETICE.

_____/____, ____ de _____ de 2021.

Atenciosamente,

ASSINATURA / CARIMBO DE CNPJ

(legível)

Empresa:

Endereço:

Telefone(s):

CNPJ:

Representante Legal:

