ANEEL
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA

ESTUDO TÉCNICO PRELIMINAR Nº 007/2020-SGI/ANEEL

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO E TECNOLÓGICAS DA ANEEL E REQUISITOS DA SOLUÇÃO DE TIC DEMANDADA

1.1 Definição e especificação das necessidades de negócio

1.1.1 A ocorrência de ataques cibernéticos contra diversas organizações públicas e privadas nacionais e internacionais vem se intensificando nos últimos anos. A eventual alta rentabilidade do crime cibernético acompanhada pela dificuldade da identificação de seus autores e a digitalização cada vez mais avançada das operações corporativas torna o risco cibernético cada vez mais relevante para as organizações.

1.1.2 Nesse sentido, no ano de 2020, o panorama de ameaças cibernéticas vem apresentando um expressivo aumento do número de ataques cibernéticos com emprego de ameaças avançadas que exploram vulnerabilidades existentes em pessoas, processos e tecnologias do ambiente computacional das organizações para adentrar nas redes corporativas e causar a indisponibilidade de sistemas de TI, paralisação de atividades e perdas definitivas dos dados eletrônicos armazenados caso não sejam atendidas as condições impostas pelos criminosos virtuais.

1.1.3 Essa ameaça, conhecida como ransomware, é uma categoria de software malicioso (malware) que ao penetrar o ambiente computacional das organizações e se proliferar pela sua rede corporativa realiza a criptografia dos arquivos eletrônicos dispostos nos discos das estações de trabalho, dos servidores físicos e virtuais, dos sistemas de armazenamento de arquivos corporativos (servidores de arquivos), dos sistemas de bancos de dados e, sobretudo, dos sistemas de backup de dados, este último considerado a última linha de defesa contra ataques cibernéticos.

1.1.4 Com isso, os arquivos eletrônicos, ao serem criptografados pelo ransomware, são impossibilitados de serem abertos ou lidos pelos colaboradores e pelos demais sistemas internos da organização

comprometendo-se imediatamente a disponibilidade dos serviços computacionais e das informações necessárias ao trabalho dos colaboradores. Ao final de todo esse processo de criptografia dos dados, o malware disponibiliza um comunicado na tela das estações e dos sistemas atingidos informando a necessidade de pagamento de um resgate ao autor do ataque, normalmente em criptomoedas, para obtenção da chave de descriptografia que reverte todo o processo.

1.1.5 Tal cenário caótico de "sequestro de dados eletrônicos", paralisia de operações e possível perda de dados foi vivido recentemente por várias empresas internacionais (HONDA, HYDRO, GARMIN, CANON, JOHANNESBURG CITY POWER, TELECOM ARGENTINA), por algumas empresas brasileiras do Setor Elétrico brasileiro públicas e privadas (ENEL, ENERGISA, LIGHT, EDP, EPE, entre outras) e, mais recentemente, por importante órgão público – STJ, onde o valor monetário do resgate estabelecido pelos criminosos foi da ordem de milhões de reais. Em alguns casos, o valor do resgate era aumentado exponencialmente em prazo inferior a vinte e quatro horas.

1.1.6 Várias dessas empresas citadas, ao optarem pela sensata decisão de não pagarem o resgate, pois o pagamento não garante que o criminoso disponibilizará a chave de descriptografia nem tampouco recomenda-se tal procedimento para que não seja fomentado o crime cibernético em questão, acabaram sofrendo paralização de suas atividades administrativas por vários dias enquanto recuperavam seus dados e sistemas por meio da restauração de cópias de segurança realizadas em mídias externas (fitas magnéticas) num processo manual, iterativo, demorado, custoso financeiramente e extremamente laboroso, uma vez que os dados guardados nos sistemas de backup corporativo foram comprometidos.

1.1.7 Ressalta-se que durante esse processo de recuperação, os dados críticos recentes normalmente são perdidos por não terem sido ainda armazenados em fitas magnéticas, mas apenas nos discos locais dos sistemas de backup da organização que não possuem estratégias e recursos de segurança cibernética suficientes para evitar a contaminação contra ransomwares.

1.1.8 Não obstante à existência de diversas soluções de segurança cibernética empregadas na proteção do ambiente computacional das organizações, tais como firewalls, antispam e antivírus, seguindo a estratégia de defesa em profundidade ou defesa em camadas, os ataques de ransomwares são normalmente efetuados por criminosos virtuais ou grupos organizados especializados que empregam modernas técnicas, táticas e procedimentos de ataques planejados que não são, em virtude disso, facilmente detectados pelos mecanismos dessas soluções.

1.1.9 Com isso, diante desse contexto de aumento de ataques cibernéticos com uso de malwares destrutivos (ransomwares) e as graves consequências que eles podem trazer à integridade e disponibilidade das informações da ANEEL verificou-se a necessidade de contratação de uma solução de TI específica para proteção de cópias de segurança dos dados mais críticos da Agência contra este tipo de ameaça visando evitar, em caso de concretização do ataque, a perda definitiva desses dados e, ao mesmo tempo, permitir a recuperação do ambiente computacional crítico em menor tempo, custo e esforço, garantindo-se dessa forma a resiliência das atividades da Agência.

1.1.10 Em função disso, no dia 15 julho de 2020, foi realizada a 3ª Reunião Ordinária do CGI da ANEEL onde foi apresentado o panorama de ameaças em questão e as ações de reforço operacionais de segurança cibernética do ambiente computacional da Agência propostas e em andamento, entre elas, a proposição de contratação de solução de backup seguro contra ataques de ransomwares.

1.1.11 Em 16 de setembro de 2020, essa demanda foi mais bem detalhada aos membros integrantes da CGI por ocasião da 4 ª Reunião Ordinária e deliberada pela aprovação de sua continuidade pelo referido Comitê (Documento SICNET 48573.000011/2020-00).

1.1.12 As seguintes orientações e iniciativas estratégias consubstanciadas nos Instrumentos Formais de Gestão da Agência (PDTI e EGD/PTD) foram utilizados como referência para esta contratação:

1.1.12 OE15 - Modernizar a infraestrutura e soluções de tecnologia da informação (PDTI);

1.1.12 OETI10 - Avançar na modernização da infraestrutura de TI (PDTI);

1.1.12 OETI11 - Desenvolver a segurança da informação em nível corporativo (PDTI);

1.1.12 IETI11.1 - Estabelecer diretrizes institucionais para a segurança da informação (PDTI);

1.1.12 OE11 - Garantia da segurança das plataformas de governo digital e de missão crítica (EGD/PTD 2020/2022);

1.1.13 Além disso, convém destacar que o Decreto 10.522, de 5 de fevereiro de 2020, que aprovou a Estratégia Nacional de Segurança Cibernética - E-Ciber, denominada de "*orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023*" prevê, entre os seus objetivos estratégicos, um relacionado diretamente com o propósito da contratação em questão: "*Aumentar a resiliência brasileira às ameaças cibernéticas*".

1.1.14 Portanto, busca-se, por meio dessa contratação o atendimento das seguintes necessidades de negócio da ANEEL:

1.1.14 Garantir a salvaguarda das cópias de segurança das informações eletrônicas críticas da Agência contra infecções e perdas definitivas causadas por ataques cibernéticos destrutivos (ransomwares);

1.1.14 Garantir o fornecimento de infraestrutura com recursos tecnológicos de segurança para as operações críticas de TI da Agência adequados ao panorama atual de ameaças cibernéticas destrutivas (ransomwares);

1.1.14 Garantir a resiliência cibernética dos dados e serviços críticos de TI da Agência em caso de desastres causados por ataques virtuais destrutivos (ransomwares);

1.1.14 Operacionalizar as disposições gerais que tratam da continuidade e recuperação de desastres estabelecidas na Política de Segurança da Informação da ANEEL (Norma de Organização ANEEL nº 012) e contidas na NC 06/IN01/DSIC/GSIPR, que estabelece as diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

1.2 Definição e especificação das necessidades tecnológicas

1.2.1 **A solução de backup atual da ANEEL**, que para fins desse estudo será denominada de **BACKUP PRIMÁRIO**, é composta pela seguinte composição de hardwares e softwares:

1.2.1 **Software de Backup -** marca Dell EMC modelo "*Networker*" contida na suíte de software "*Dell Data Protection Suite*";

1.2.1 **Hardware de Backup** - Subsistema de armazenamento do tipo appliance do fabricante "*Dell EMC Data Domain 6800*";

1.2.1 **Demais componentes** - Subsistemas de armazenamento para fins de arquivamento e biblioteca de fitas também do fabricante DELL;

1.2.2 Isto posto, foram mapeadas as seguintes necessidades tecnológicas gerais para atendimento das necessidades de negócio levantadas na seção anterior cujos requisitos tecnológicos serão detalhados na próxima seção "item 1.4 – Requisitos técnicos e funcionais da Solução de TIC"

1.2.3 Arquitetura do ambiente de contingência:

1.2.3 Prover um ambiente de contingência (réplica de backup) destinado à sincronização automatizada dos dados de backup dos sistemas críticos da ANEEL contidos na solução de **backup primário da ANEEL**, onde a solução deverá:

I. Ser totalmente compatível à solução de **backup primário da ANEEL**;

II. Armazenar de forma protegida do acesso pela rede corporativa os dados de backup dos sistemas críticos da ANEEL em dispositivo de armazenamento isolado fisicamente por meio do emprego de mecanismo automatizado de desconexão (network air-gap);

III. Reduzir a exposição a ataques cibernéticos por meio de uso de dispositivo com arquitetura endurecida (hardened) e que possua uma estratégia de atualização e patches consistentes para os componentes da solução (appliance de backup);

IV. Mitigar o risco de acesso indevido ao dispositivo de armazenamento por meio do controle de acesso administrativo com uso credenciais de segurança separadas e que possibilite o uso de múltiplos fatores;

V. Mitigar o risco de corrupção de dados usando mecanismos que garantam a imutabilidade do software de backup utilizado na solução;

VI. Mitigar o risco de alteração dos dados de backup armazenados (WORM – "*write once read many*");

VII. Detectar a atividade de ransomware nos dados com base em mecanismos de lógica analítica e aprendizagem automática;

VIII. Detectar anomalias específicas nos dados causadas por atividade de ransomware e alertar rapidamente os administradores de TI enquanto os dados estão sendo submetidos ao processo de backup;

IX. Mitigar o risco de contaminação do dispositivo de armazenamento de backup por ransomware que se prolifera utilizando protocolos de comunicação Server Message Block (SMB) e Network File System (NFS);

X. Disponibilizar ferramentas periciais para detectar, diagnosticar e corrigir ataques cibernéticos de ransomware em andamento;

XI. Aumentar a velocidade de recuperação usando métodos de detecção e análise que identifiquem rapidamente os dados afetados e a associem ao melhor ponto de recuperação;

XII. Acelerar a recuperação utilizando dispositivo de armazenamento de backup que contenha área de armazenamento específica antes de mover os dados e sistemas recuperados para a produção;

1.2.4 Serviços Agregados da Contratação:

1.2.4 Deverá contemplar serviços agregados de implementação da solução (instalação e configuração) e serviços de suporte técnico especializado (garantia e suporte técnico) para que sejam realizados além de atendimentos preventivos e corretivos na solução, definição e implementação na solução de planejamento de backup e recuperação dos serviços críticos da ANEEL por meio também de testes de recuperação conforme as boas práticas do fabricante e de forma a trazer um melhor aproveitamento do espaço disponibilizado no armazenamento da solução e mantendo-se o ambiente preparado para o evento de ataque.

1.3 Especificação de Requisitos da Solução de TI

1.3.1 Requisitos de Capacitação:

1.3.1 Não foram identificados requisitos de capacitação para essa contratação.

1.3.2 Requisitos de Tecnologia:

1.3.2 Os equipamento e softwares a serem utilizados devem ser compatíveis com a atual plataforma tecnológica utilizada na Agência, sobretudo com o ambiente computacional do **backup primário da Agência**, com vistas a não impactar nas operações do datacenter da Agência, e:

1.3.2.1.1 A solução deverá contemplar todos os componentes necessários ao seu pleno funcionamento compatível com os equipamentos e soluções contidas no datacenter da ANEEL (ex: fibras óticas, patch cords, transceivers, PDUs, tomadas elétricas, entre outros).

1.3.2.1.2 As licenças entregues deverão garantir o acesso a novas versões dos produtos relacionados, bem como todas as atualizações de segurança e pacotes de correção de problemas, durante todo o período contratado;

1.3.3 Requisitos Temporais e de Local de Execução:

1.3.3 A CONTRATADA deverá entregar os produtos/serviços conforme cronograma abaixo, sendo que os prazos estabelecidos serão contados a partir da data de assinatura do Contrato.

Evento	Descrição	Prazo	Responsável
1	Início da Vigência do Contrato	-	ANEEL e CONTRATADA
2	Reunião inicial	Em até 5 (cinco) dias corridos, contados a partir do evento 01	ANEEL e CONTRATADA
3	Entrega do Plano de Instalação	Em até 15 (quinze) dias corridos, contados a partir do evento 02.	CONTRATADA
4	Avaliação do Plano de Instalação	Em até 10 (dez) dias corridos, contados a partir do evento 03	ANEEL
5	Entrega dos produtos, equipamentos e softwares.	Em até 60 (sessenta) dias corridos, contados a partir do evento 02	CONTRATADA
6	Emissão do Termo de Recebimento Provisório de Entrega dos Equipamentos e Softwares	Em até 10 (dez) dias corridos, contados a partir do evento 05	ANEEL

7	Instalação, configuração e operacionalização dos produtos, equipamentos e softwares.	Em até 90 (noventa) dias corridos, contados a partir do evento 01	CONTRATADA
8	Emissão do Termo de Recebimento Definitivo de Entrega dos Equipamentos e Softwares	Em até 10 (dez) dias corridos, contados a partir do evento 07	ANEEL

1.3.3 A entrega deverá ser realizada nas dependências da ANEEL localizadas na SGAN 603 Modulos "I" e "J" - Asa Norte, Brasília - DF, 70830-110, destinada ao Núcleo de Segurança da Informação da Superintendência de Gestão Técnica da Informação - SGI. O email para contato é o infrati@aneel.gov.br e o telefone é o (61)2192-8671

1.3.4 Requisitos de Segurança:

1.3.4 Todo acesso on-site ou remoto necessário ao suporte da solução deverá ser previamente autorizado pela ANEEL e respeitar as normas vigentes da segurança da informação (Norma de organização da ANEEL nº 012) mantendo-se a confidencialidade de qualquer informação sigilosa da ANEEL obtida durante a contratação.

1.3.4 Após a assinatura do contrato, os profissionais responsáveis pela execução dos serviços deverão assinar o Termo de Ciência de Confidencialidade e Manutenção de Sigilo, comprometendo-se a preservar as informações a que tiverem acesso em virtude dos serviços prestados.

1.3.4 Os equipamento e softwares a serem utilizados devem ser compatíveis com a atual plataforma tecnológica utilizada na Agência, sobretudo com o ambiente computacional do **backup primário da Agência**, com vistas a não impactar nas operações do datacenter ou em perdas de dados durante a execução do Contrato.

1.3.5 Requisitos Legais:

1.3.5 O fornecimento da solução deverá levar em consideração os requisitos constantes da INSTRUÇÃO NORMATIVA Nº 01 da SGD/ME, de 04 de abril de 2019.

1.3.6 Requisitos de Manutenção, Garantia e Suporte Técnico da Solução

1.3.6 A solução deverá possuir garantia técnica durante o período integral da contratação;

1.3.6 Durante o período de garantia, deverá ser prestado serviço de suporte técnico, com atendimento remoto em regime integral (24 (vinte e quatro) horas por dia e 7 (sete) dias por semana);

1.3.6 Em complemento serão exigidos serviços de suporte técnico especializado visando o planejamento e execução de configurações de política de backup de sistemas críticos, realização de testes de recuperação de desastres, entre outras atividades;

1.3.6 Os requisitos de manutenção, garantia e suporte técnico estão detalhados na seção Especificações Técnicas da Solução de TI deste documento.

1.3.7 Requisitos Sociais, Ambientais e Culturais:

1.3.7 Serão exigidos requisitos de compressão e/ou desduplicação de dados, com o intuito de reduzir o espaço ocupado em dispositivos de armazenamento digital (storages e fitas magnéticas);

1.3.7 Todos os softwares e atualizações deverão ser disponibilizadas para a ANEEL por meio eletrônico, pela internet, de forma a evitar o impacto da produção de CD/DVD sobre recursos naturais.

1.3.7 Toda a documentação de software e base de conhecimento deverá estar disponível na internet, de forma a evitar impacto sobre recursos naturais decorrentes de produção de material de impressão, de pacotes e de desfazimento futuro.

1.3.8 Especificações técnicas da solução de TIC

1.3.8 Para a montagem do ambiente de contingência (réplica) do **backup primário da ANEEL** com funcionalidades específicas de segurança cibernética contra ataques de ransomwares, deverão ser

incluídos os seguintes componentes para a solução tecnológica em questão (conforme descrito na seção de “estudo da solução a ser contratada” deste documento):

I. **Hardware de Backup**: para fins de armazenamento otimizado dos dados replicados da solução de **backup primário da ANEEL**;

II. **Software de Backup**: para fins de gerenciamento e orquestração das atividades de replicação de dados da solução de backup primário;

III. **Software de Detecção e Análise de Malwares (ransomwares)**: para fins de detecção da presença de ransomware nos dados de backup replicados, bem como na implementação de mecanismos de alertas e recuperação acelerada conforme informados na seção anterior;

IV. **Software de microsegmentação de redes**: para fins de realização do isolamento definido por software da rede corporativa dos servidores virtuais que compõem o ambiente de contingência (réplica).

V. **Hardware de Servidores**: os softwares que compõem esta solução deverão ser instalados em máquinas virtuais hospedadas respectivamente em servidores físicos com características de segurança específica do ambiente de contingência (ex: isolamento);

VI. **Hardware de comunicação LAN (switch):** para fins de interconectividade dos componentes físicos da solução com a solução de backup primário da ANEEL.

1.3.8 **Hardware de backup (appliance)**

1.3.8.1 O appliance de backup em disco de réplica terá as finalidades específicas de armazenar uma réplica segura dos dados do equipamento de backup primário;

1.3.8.2 O appliance de backup em disco de réplica (secundário) deve ser do mesmo fabricante e modelo igual ou superior ao equipamento Dell EMC DATA DOMAIN modelo DD6800 atualmente instalado nas dependências da ANEEL;

1.3.8.3 Não será permitida oferta de soluções que não sejam compatíveis e permita receber os dados de maneira nativa do atual equipamento em uso;

1.3.8.4 O equipamento deve ser fornecido em gabinete (rack), do próprio fabricante, no padrão de 19" (dezenove polegadas), com no mínimo 40U (quarenta unidades) de altura;

1.3.8.5 Deverá possuir licenciamento para capacidade mínima de 120TB úteis sem considerar ganhos com desduplicação e compressão de dados;

1.3.8.6 O appliance de backup primário da ANEEL possui as seguintes especificações básicas:

1.3.8.6.1 Marca: Dell EMC

1.3.8.6.2 Modelo: Data Domain DD6800

1.3.8.6.3 Número de Sério: FC500174600002

1.3.8.6.4 Capacidade Total líquida: 260TB

1.3.8.6.5 Controladora de processamento composta por:

1.3.8.6.5.1 01 (uma) controladora de processamento modelo DD6800

1.3.8.6.5.2 02 (dois) processadores de 08 (oito) núcleos, com arquitetura x86;

1.3.8.6.5.3 192GB de Memória RAM

1.3.8.6.5.4 Módulo NVRAM 8GB

1.3.8.6.5.5 Fontes de alimentação e ventiladores redundantes

1.3.8.6.5.6 06 (seis) discos SAS-SDD de 800GB cada

1.3.8.6.5.7 04 (quatro) portas Ethernet 10Gbps (Base-T)

1.3.8.6.5.8 08 (oito) portas Ethernet 10Gbps otico padrão SFP+

1.3.8.6.5.9 02 (duas) portas Fiber Channel (FC) 16Gbps padrão SFP+;

1.3.8.6.5.10 Gavetas de discos composta por:

1.3.8.6.5.11 Módulo de alimentação redundantes;

1.3.8.6.5.12 90 (noventa) discos SAS de 4TB brutos cada.

1.3.8.6.6 Licenciamento de Software para toda capacidade instalada:

1.3.8.6.6.1 DD Boost

1.3.8.6.6.2 Encryption

1.3.8.6.6.3 Replication

1.3.8.6.6.4 Retention-Lock-Compliance

1.3.8.6.6.5 Retention-Lock-Governance

1.3.8.6.6.6 VTL

1.3.8.6.6.7 DD Cloud Tier

1.3.8.7 Os equipamentos fornecidos devem ser instalados e configurados no ambiente da CONTRATANTE, por meio de profissional técnico do fabricante ou devidamente certificado pela fabricante dos equipamentos. A CONTRATADA deverá apresentar as devidas certificações no momento da instalação.

1.3.8.8 Os equipamentos e componentes fornecidos deverão possuir garantia genuína do fabricante, na modalidade “24x7x365”, com atendimento “on-site”, com cobertura para substituições de peças e componentes de hardware que venham a apresentar falha durante o período de garantia contratado.

1.3.8.9 Todos os componentes de hardware e software devem contemplar **60 (sessenta) meses de garantia e suporte técnico do próprio Fabricante**, contada a partir do recebimento definitivo do produto, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

1.3.9 Software de backup

1.3.9.1 Uma vez que a ANEEL possui vigente o licenciamento do software de backup presente na solução de backup primário (Dell EMC Networker), deverá ser realizada a expansão desse software para montagem do ambiente de contingência.

1.3.9.2 Fornecimento de Licença de Uso por Processador (por socket) do Software Gerenciador de Backup DELL EMC NETWORKER, intitulada “DATA PROTECTION SUITE FOR BACKUP” ou equivalente caso esta tenha oficialmente sofrido mudança de nomenclatura por parte do fabricante;

1.3.9.3 A licença acima descrita deve ser fornecida em conjunto com qualquer outra licença do produto “DELL EMC Networker” que porventura seja necessária à sua ativação ou funcionamento;

1.3.9.4 A licença deve permitir quantidade ilimitada de dados de backup, de volume de dados nos servidores/serviços de origem, e de volume de dados armazenados através da solução de backup.

1.3.9.5 O licenciamento ofertado deve ser totalmente compatível com o software Dell EMC NETWORKER já atualmente instalado na ANEEL;

1.3.9.6 Não será aceito modelo de licenciamento que não seja prática de mercado usual do fabricante. Informações do modelo de licenciamento ofertado devem constar em documentação oficial da fabricante.

1.3.9.7 As licenças, objeto desta licitação, poderão ser instaladas e utilizadas tanto em parque tecnológico próprio quanto em de terceiros, desde que em uso pela CONTRATANTE.

1.3.9.8 Todos os Part numbers supracitados devem contemplar garantia de 60 (sessenta) meses e suporte técnico do próprio fabricante pelo mesmo período, contada a partir do recebimento definitivo do produto, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

1.3.9.9 O suporte técnico do fabricante deverá fornecer direito de atualização contínua dos produtos licenciados, assim como novas versões e patches de atualização;

1.3.9.10 Deverá ser disponibilizada pelo FABRICANTE uma central de atendimento, 24 horas por dia, 7 dias por semana, todos os dias do ano.

1.3.9.11 O atendimento do suporte técnico pelo FABRICANTE deverá ser em horário integral, TELEFÔNICO e ELETRÔNICO, na modalidade 24x7x365;

1.3.10 Software de firewall e microssegmentação de rede

1.3.10.1 Uma vez que a ANEEL possui vigente o licenciamento do software de microsegmentação de redes (VMware NSX), deverá ser realizada a expansão desse software para montagem do ambiente de contingência.

1.3.10.2 Deve ser fornecido licenciamento de uso por processador (por socket) do software de virtualização de redes VMware NSX Data Center Advanced, intitulada “NX-DC-ADEPL-UG-C” ou equivalente caso esta tenha oficialmente sofrido mudança de nomenclatura por parte do fabricante;

1.3.10.3 O licenciamento ofertado deve ser totalmente compatível com o software “VMware NSX Data Center Advanced” já atualmente instalado na ANEEL;

1.3.10.4 Não será aceito modelo de licenciamento que não seja prática de mercado usual do fabricante. Informações do modelo de licenciamento ofertado devem constar em documentação oficial da fabricante.

1.3.10.5 As licenças, objeto desta licitação, poderão ser instaladas e utilizadas tanto em parque tecnológico próprio quanto em de terceiros, desde que em uso pela CONTRATANTE.

1.3.10.6 Todos os Part numbers supracitados devem contemplar garantia de 60 (sessenta) meses e suporte técnico do próprio fabricante pelo mesmo período, contada a partir do recebimento definitivo do produto, sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

1.3.10.7 O suporte técnico do fabricante deverá fornecer direito de atualização contínua dos produtos licenciados, assim como novas versões e patches de atualização;

1.3.10.8 Deverá ser disponibilizada pelo FABRICANTE uma central de atendimento, 24 horas por dia, 7 dias por semana, todos os dias do ano.

1.3.10.9 O atendimento do suporte técnico pelo FABRICANTE deverá ser em horário integral, TELEFÔNICO e ELETRÔNICO, na modalidade 24x7x365;

1.3.11 Software de detecção e análise de malwares (ransomwares)

1.3.11.1 Fornecimento de Licença de Uso por Capacidade de origem (Terabytes) do módulo CyberSense do software Gerenciador de Backup DELL EMC NETWORKER intitulada “DATA PROTECTION SUITE FOR BACKUP” ou equivalente caso esta tenha oficialmente sofrido mudança de nomenclatura por parte do fabricante;

1.3.11.2 O módulo CyberSense deve permitir ser integrado de forma nativa com software Dell EMC Networker em uso pela CONTRATANTE;

1.3.11.3 O módulo deve verificar a integridade dos dados de backup do software Dell EMC Networker e determinar se existe alguma corrupção ou foi comprometido por algum malware ou ransomware;

1.3.11.4 A solução deve identificar a corrupção de dados, incluindo criptografia, ransomware, destruição e corrupção lenta dos arquivos copiados;

1.3.11.5 Possuir ferramentas forenses e fazer uso de métodos analíticos de aprendizado de máquina (Machine Learning) com no mínimo 100 estatísticas para encontrar arquivos corrompidos e diagnosticar o vetor de ataque a partir da imagem de backup;

1.3.11.6 A solução deve possuir a capacidade de analisar as cópias de backup sem restaurar os dados de backup;

1.3.11.7 O módulo de análise deve realizar a varredura no conteúdo completo dos arquivos (full-content) incluindo metadados;

1.3.11.8 O módulo deve monitorar arquivos e bancos de dados para determinar se ocorreu um incidente com base na corrupção de dados;

1.3.11.9 Deve fazer a varredura em arquivos de bancos de dados como: Oracle, DB2 e Microsoft SQL.

1.3.11.10 Deve monitorar a integridade dos dados de backup, enviar relatórios e alertas quando ocorrem mudanças que indicam um incidente cibernético;

1.3.11.11 Capacidade de se integrar com o software Dell EMC Networker e restaurar rapidamente o último backup válido;

1.3.11.12 A solução deve operar completamente offline e apartada da rede de produção, exceto ao receber atualizações da réplica dos backups;

1.3.11.13 Deve possuir módulo capaz de gerenciar as regras de replicação controlada garantindo a réplica segura com “air-gap” de comunicação com o equipamento Dell EMC Data Domain primário (produção) e secundário (réplica);

1.3.11.14 A solução deve gerenciar os processos de proteção do equipamento de réplica para desligar portas TCP e serviços não utilizados, assim como ativar o bloqueio e imutabilidade dos dados quando necessário;

1.3.11.15 A solução deve usar criptografia para transferir dados entre o equipamento Dell EMC Data Domain primário (produção) e secundário (réplica);

1.3.11.16 Deve gerenciar e aplicar regras de imutabilidade (WORM) nas imagens de backup consideradas livres de qualquer infecção ou corrupção;

1.3.11.17 Deve possuir console gráfica capaz de gerenciar e informar o status das imagens de backup, assim como a última cópia válida;

1.3.11.18 A solução deve fornecer a capacidade de manter várias cópias de dados de maneira segura.

1.3.11.19 O suporte técnico do fabricante deverá fornecer direito de atualização contínua dos produtos licenciados, assim como novas versões e patches de atualização;

1.3.11.20 Deverá ser disponibilizada pelo FABRICANTE uma central de atendimento, 24 horas por dia, 7 dias por semana, todos os dias do ano.

O atendimento do suporte técnico pelo FABRICANTE deverá ser em horário integral, TELEFÔNICO e ELETRÔNICO, na modalidade 24x7x365;

1.3.12 Hardware de comunicação de rede LAN (switch)

1.3.12.1 O equipamento deve ser compatível e suportado nativamente com o switch de rede Dell EMC S5048F-ON em uso na ANEEL;

1.3.12.2 O equipamento deve possuir no mínimo 24 (vinte e quatro) portas 1/10/25 Gigabit Ethernet SFP28;

1.3.12.3 As portas devem ser do tipo auto-sense, identificando a velocidade de acordo com o transceiver inserido, sem a necessidade de configurações manuais;

1.3.12.4 Deve ocupar no máximo 1 (uma) unidade de rack (1 RU);

1.3.12.5 Deve ser instalável em rack padrão de 19”, sendo que deverão ser fornecidos os respectivos kit’s de fixação;

1.3.12.6 As portas SFP28 devem suportar transceivers dos padrões SFP+ 10GBase-SR, 10GBase-LR, 10GBase-ER, SFP 1000Base-SX, 1000Base-LX, 1000Base-ZX e 1000Base-T e cabos Direct Attach Cable (DAC);

1.3.12.7 Deve ser fornecido com pelo menos 24 (vinte e quatro) transceivers 25GBase-YY. Os transceivers fornecidos deverão ser do mesmo fabricante do switch;

1.3.12.8 Possuir no mínimo 04 (quatro) portas 100 Gigabit Ethernet QSFP28 com suporte a velocidades de 40 e 100 Gigabit Ethernet.

1.3.12.9 Deve suportar transceivers padrões 40GBase-SR4, 40GBase-LR4;

1.3.12.10 Deve suportar transceivers padrão 100GBase-SR4 e 100GBase-LR4;

1.3.12.11 Cabos Direct Attach Cable (DAC);

1.3.12.12 Deve ser fornecido com pelo menos 04 (quatro) transceivers 40GBase-YY. Os transceivers fornecidos deverão ser do mesmo fabricante do switch;

1.3.12.13 Deve possuir matriz de comutação com capacidade de pelo menos 4 Tbps;

1.3.12.14 Deve possuir capacidade mínima de 1.5 Bpps de Throughput;

1.3.12.15 Deve possuir buffer mínimo de 32 MB;

1.3.12.16 Deve possuir latência menor ou igual a 900 nanosegundos;

1.3.12.17 Deve possuir capacidade para no mínimo 160.000 endereços MAC;

1.3.12.18 Deve implementar tabela ARP com até 128.000 entradas;

1.3.12.19 Deve suportar a Jumbo frames de no mínimo 9000 bytes;

1.3.12.20 Deve possuir no mínimo 1 (uma) porta de console com conector RJ-45;

1.3.12.21 Deve possuir no mínimo 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management);

1.3.12.22 Deve ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

1.3.12.23 Deve possuir fontes de alimentação redundantes internas ao equipamento com ajuste automático de tensão 110 ou 220 volts;

1.3.12.24 O equipamento deverá ter ventiladores redundantes com opção de fluxo de ar frente para trás ou trás para frente (front-to-back ou back-to-front).

1.3.12.25 As fontes e ventiladores devem ser capazes de serem trocados com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable) e devem ser redundantes;

1.3.12.26 O equipamento deve ser específico para o ambiente de Datacenter com comutação de pacotes de alto desempenho;

1.3.12.27 Deve ser um equipamento homologado pela Agência Nacional de Telecomunicações (Anatel);

1.3.12.28 Funcionalidades Gerais

1.3.12.29 Deve possuir LEDs, por porta, que indiquem a integridade e atividade do link;

1.3.12.30 Deve possuir LEDs do tipo blue beacon para identificação do switch e da porta a ser acessada, para facilitar a manutenção;

1.3.12.31 A solução deve implementar e prover arquitetura de rede de data center utilizando a arquitetura “spine - leaf”, tendo o VxLAN como plano de dados (“data-plane”) e BGP EVPN para o plano de controle (“control-plane”).

1.3.12.32 Deve possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);

1.3.12.33 Deve ser gerenciável via SSHv2;

1.3.12.34 O switch deve ter no mínimo criptografia FIPS 140-2 comprovado pelo NIST;

1.3.12.35 O switch suportar o padrão X.509v3 para certificados digitais;

1.3.12.36 Deve permitir o espelhamento de uma porta e de um grupo de portas para uma porta especificada;

1.3.12.37 Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em um switch remoto no mesmo domínio L2 ou em outro domínio L2 através de tunelamento;

1.3.12.38 Deve implementar Netflow, sFlow ou similar;

1.3.12.39 Deve suportar SDN ao menos com Openflow 1.3;

1.3.12.40 Deve ser gerenciável via SNMPv3;

1.3.12.41 Deve implementar o protocolo Syslog para funções de “logging” de eventos;

1.3.12.42 Deve implementar o protocolo NTPv4 ou SNTP;

1.3.12.43 Deve suportar autenticação RADIUS sobre TLS;

1.3.12.44 Deve suportar autenticação TACACS+;

1.3.12.45 Deve implementar controle de acesso por porta (IEEE 802.1x);

1.3.12.46 Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4 ou IPv6 de origem e destino, portas TCP e UDP de origem e destino e endereços MAC de origem e destino;

1.3.12.47 Deve possuir controle de broadcast, multicast e unicast por porta;

1.3.12.48 Deve implementar pelo menos uma fila de saída com prioridade estrita (SP Strict Priority) por porta e divisão ponderada (WRED, WRR ou similar) de banda entre as demais filas de saída;

1.3.12.49 Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

1.3.12.50 Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

1.3.12.51 Deve implementar classificação de tráfego baseada em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;

1.3.12.52 Deve formar um virtual switch, de forma que os dois possam ser vistos como uma entidade única, logicamente. Esta funcionalidade pode ser provida através de:

1.3.12.52.1 Suporte à funcionalidade de agregação de portas multi-chassi, através da criação de redundância ativa/ativa livre de loop e sem utilização de protocolo Spanning Tree, conforme as tecnologias MLAG, MC-LAG, M-LAG, Virtual Link Trunking, Multi-Chassis EtherChannel ou equivalentes

1.3.12.53 Deverão ser fornecidos todos os componentes necessários para garantia da alta disponibilidade, incluindo todos os módulos e/ou cabos/transceivers para interconexão dos equipamentos, bem como as licenças necessárias, caso aplicável;

1.3.12.54 Os equipamentos quando virtualizados deverão possuir processamento local de modo a não existir tempo de convergência em caso de falha de um dos equipamentos do sistema virtualizado;

1.3.12.55 Funcionalidades de Camada 2

1.3.12.55.1 Deve implementar até 4.000 VLANs Ids conforme definições do padrão IEEE 802.1Q;

1.3.12.55.2 Deve suportar VLANs dinâmicas. Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;

1.3.12.55.3 Deve implementar “VLAN Trunking” conforme padrão IEEE 802.1Q nas portas Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados.

1.3.12.55.4 Deve implementar a funcionalidade de “Link Aggregation(LAGs)” conforme padrão IEEE 802.3ad;

1.3.12.55.5 Deve suportar no mínimo 100 grupos por switch com até 16 portas por LAG (IEEE 802.3ad);

1.3.12.55.6 Deve implementar o padrão IEEE 802.1d, IEEE 802.1s e IEEE 802.1w;

1.3.12.55.7 Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree;

1.3.12.55.8 Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

1.3.12.55.9 Deve implementar o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP) e sua extensão LLDP-MED, permitindo a descoberta dos elementos de rede vizinhos;

1.3.12.55.10 O equipamento deve suportar funcionalidade de virtualização em camada 2 de modo a suportar diversidade de caminhos em camada 2 e agregação de links entre 2 switches distintos (Layer 2 Multipathing);

1.3.12.55.11 Suporte a DCB (Data Center Bridging), com suporte aos protocolos Priority-based flow control (PFC – IEEE 802.1Qbb), Enhanced Transmissions Selections (ETS – IEEE 802.1Qaz) e DCBx;

1.3.12.56 Funcionalidades de Roteamento

1.3.12.56.1 Deve possuir roteamento nível 3 entre VLANs;

1.3.12.56.2 Deve implementar protocolos de roteamento dinâmico OSPFv3;

1.3.12.56.3 Deve implementar protocolos de roteamento dinâmico BGPv4 e BGPv6;

1.3.12.56.4 Deve ter suporte a 120.000 (cento e vinte mil) rotas IPv4;

1.3.12.56.5 Deve ter suporte a 60.000 (sessenta mil) rotas IPv6;

1.3.12.56.6 Deve trabalhar simultaneamente com protocolos IPv4 e IPv6;

1.3.12.56.7 Deve implementar VRF ou VRF-Light com suporte a no mínimo 500 instâncias;

1.3.12.56.8 Deve implementar Policy Based Routing;

1.3.12.56.9 Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol) v3;

1.3.12.56.10 Os equipamentos devem possuir garantia de 60 (sessenta) meses com um período de disponibilidade para chamada de manutenção de 24 horas por dia, 7 dias por semana com prazo para envio de peças até o próximo dia útil subsequente à abertura do chamado técnico;

1.3.12.56.11 A CONTRATANTE poderá abrir chamados de manutenção diretamente no fabricante do item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software;

1.3.12.56.12 A abertura de chamados poderá ser realizada através de telefone 0800 do fabricante, através da página da WEB do fabricante ou através de endereço de e-mail do fabricante;

1.3.12.56.13 A abertura de chamados através de telefone 0800 deverá ser realizada inicialmente em português;

1.3.12.56.14 Deverá ser garantido à CONTRATANTE o pleno acesso ao site do fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

1.3.12.56.15 Durante o período de suporte técnico, devem ser disponibilizados e instalados, sem ônus à contratante, todas as atualizações de software e firmware para os equipamentos, quando for necessário;

1.3.12.56.16 O licitante deve apresentar os códigos/sku's/part number do serviço de garantia do fabricante dos equipamentos, sendo que todos os equipamentos deverão ser previamente registrados pelo fornecedor junto ao fabricante, em nome da contratante.

1.4 Requisitos de Serviços de Implementação da solução

1.4.8 CONTRATADA deverá fornecer os seguintes serviços de entrega, instalação, e configuração de todos os componentes ofertados visando sua operacionalidade total:

1.4.1.1 Instalação física e configuração de todos os componentes ofertados;

1.4.1.2 Fornecimento de Check List para conferência do(s) equipamento(s)/componente(s)/solução entregue(s), contendo todos os itens especificados na proposta comercial e seus respectivos números de série;

1.4.1.3 Projeto executivo com a proposta de configuração e customização do(s) equipamento(s)/componente(s)/solução;

1.4.1.4 Retirada do(s) equipamento(s)/componente(s) das embalagens;

1.4.1.5 Movimentação do(s) equipamento(s)/componente(s) da sala de quarentena para a sala de produção;

1.4.1.6 Instalação física do(s) equipamento(s)/componente(s);

1.4.1.7 Cabeamento do(s) equipamento(s);

1.4.1.8 Energização do(s) equipamento(s);

1.4.1.9 Configuração inicial do(s) equipamento(s)/solução de acordo com o projeto executivo;

1.4.1.10 Transferência de conhecimento sobre o gerenciamento do(s) equipamento(s)/solução, durante pelo menos 08 horas, de forma a habilitar, no mínimo, 02 (dois) técnicos da ANEEL a operar o(s) equipamento(s);

1.4.1.11 Atualização/instalação dos softwares que compõem a solução;

1.4.1.12 Customização da solução, conforme plano de arquitetura definido em conjunto com os técnicos da ANEEL;

1.4.1.13 Caso sejam necessários testes após o processo de retirada dos equipamentos das embalagens, a CONTRATADA fica obrigada a realizar os testes em local definido pela ANEEL, executando os testes, desmontando, transportando e reinstalando o(s) equipamento(s) na sala de PRODUÇÃO.

1.4.9 A CONTRATADA fica obrigada, mediante solicitação da ANEEL, a certificar todas as condições físicas (elétricas e ambientais) da sala na qual haverá a instalação dos equipamentos adquiridos, conforme padrões estabelecidos pelos fabricantes.

1.4.10 A CONTRATADA deverá, caso necessário, adaptar e/ou construir as tomadas elétricas do(s) equipamento(s) adquirido(s), no momento da instalação, de forma que as unidades de distribuição de força atendam às exigências de disponibilidade do equipamento.

1.4.11 Fica sob responsabilidade da CONTRATADA, disponibilizar a função de abertura automática de chamados pelo equipamento para a central do fabricante, através de linha VPN (“Virtual Private network”) ou acesso seguro, visando acelerar o diagnóstico remoto em caso de erros/defeitos.

1.4.12 Os dispositivos necessários para a implementação desta funcionalidade são de responsabilidade da CONTRATADA, à exceção da linha telefônica comum ou conexão com à internet, que será fornecida pela ANEEL.

1.4.13 A CONTRATADA deverá fornecer um documento constando o Projeto Executivo, no qual descreverá a proposta de configuração e customização dos equipamentos para atender as necessidades da ANEEL.

1.4.14 É de responsabilidade da CONTRATADA instalar, configurar, formatar e customizar (visando a melhor performance possível) a solução (appliance ou hardware e software), com o acompanhamento da equipe técnica da ANEEL, visando o repasse do conhecimento, em data e horário a serem determinados pela ANEEL, preferencialmente em dia útil.

1.4.15 A CONTRATADA deve possuir e informar página da Internet na qual estejam disponíveis drivers atualizados, últimas versões de firmware e demais informações sobre detalhes técnicos dos equipamentos, sem restrições de acesso, público ou acesso via cadastramento de pessoas autorizadas pela CONTRATANTE.

1.4.16 A CONTRATADA deverá manter a ANEEL informada das versões/atualizações, correções (patches) e vulnerabilidades dos produtos contemplados neste Termo de Referência.

1.4.17 A CONTRATADA deverá fornecer novas versões/atualizações pela Internet, dos produtos constantes neste ETP sem qualquer custo adicional à ANEEL, visando garantia da compatibilidade binária e operacional destes softwares com os equipamentos adquiridos.

1.4.18 Na instalação, deverão ser contempladas/executadas, no mínimo, as seguintes atividades:

1.4.11.1 Planejamento da instalação;
1.4.11.2 Validação da matriz de compatibilidade dos componentes;
1.4.11.3 Instalação do Hardware e do Software;
1.4.11.4 Inicialização de todos os Hardware ofertados;
1.4.11.5 Verificação da Instalação;
1.4.11.6 Verificação e Atualização dos Níveis e Firmware;
1.4.11.7 Conexão física/lógica à rede da ANEEL;
1.4.11.8 Elaboração e Entrega de Documentação de Instalação e Configuração após o término dos trabalhos

.

1.4.19 Na configuração, deverão ser contempladas/executadas, no mínimo, as seguintes atividades:

1.4.12.1 Configurar os módulos e demais softwares ofertados que compõem toda solução;

1.4.12.2 Configurar as Credenciais e Acesso e Endereços de Rede;

1.4.12.3 Configurar as Interfaces de Gerenciamento Unificado;

1.4.12.4 Configurar a replicação segura entre os equipamentos Dell EMC Data Domain primário e secundário;

1.4.12.5 Apoiar a equipe de segurança da ANEEL na definição das regras de firewall virtual;

1.4.12.6 Configurar toda comunicação lógica dos equipamentos ofertados;

1.4.12.7 Ativar as Licenças e Features Adquiridas;

1.4.12.8 Criar Pools de Armazenamento e replicação no Data Domain de réplica;

1.4.12.9 Apresentar Volumes de Backup para o servidor de backup do ambiente de réplica;

1.4.12.10 Elaborar plano e configurar até 10 (dez) políticas de replicação segura;

1.4.12.11 Configurar até 10 (dez) políticas de agendamento da varredura de verificação e análise via CyberSense;

1.4.12.12 Realizar testes e execução das rotinas de validação e envio de alerta das rotinas de varredura;

1.4.12.13 Realizar testes de backup e recuperação das 10 (dez) políticas;

1.4.12.14 Elaborar documentação com procedimentos para validação e recuperação dos backups limpos de qualquer malware ou ransomware;

1.4.12.15 Elaborar documentação de Instalação e Configuração após o término dos trabalhos;

1.4.19.1 Durante a implementação da solução, o fornecedor deverá providenciar o repasse de conhecimento das ferramentas e componentes da solução ofertada à equipe técnica da ANEEL, de forma que a administração e operação seja feita de forma independente, contemplando todas as funcionalidades especificadas neste documento;

1.5 Requisitos de Serviços Especializados de Suporte

1.5.8 A CONTRATADA deverá disponibilizar pelo menos 1 (um) profissional “on-site”, de modo que a qualquer momento a CONTRATANTE poderá acioná-lo através de um chamado técnico a ser aberto via telefone, e-mail e/ou ferramenta da ANEEL para gerenciamento de chamados;

1.5.9 O pacote mínimo de horas para atender cada acionamento será de 16 (dezesseis) horas;

1.5.10 O profissional deve ser certificado e possuir experiência comprovada com os produtos DELL EMC DATA DOMAIN, EMC NETWORKER ou DATA PROTECTION SUITE utilizados no ambiente de backup da CONTRATANTE. **A CONTRATADA deverá apresentar as devidas certificações no momento da assinatura do contrato**;

1.5.11 O suporte técnico especializado poderá ser utilizado para os serviços descritos abaixo:

1.5.12 Administração preventiva e corretiva especializada, incluindo atualização de software e sustentação dos equipamentos DELL EMC DATA DOMAIN e DATA PROTECTION SUITE que fazem parte do ambiente de backup da CONTRATANTE;

1.5.13 Suporte especializado, recomendação das melhores práticas do fabricante, resolução de problemas e análise de desempenho de equipamentos e sistemas de backup existentes no ambiente da CONTRATANTE;

1.5.14 Implementação e execução técnico-operacional de projetos infraestrutura de armazenamento conforme arquitetura definida pela CONTRATANTE;

1.5.15 Implementação e sustentação de soluções de contingência de dados em equipamentos de Backup;

1.5.16 Emissão ou atualização de relatórios e documentação técnico-operacional conforme arquitetura definida pela CONTRATANTE;

1.5.17 Acompanhamento de gerenciamento do ambiente de armazenamento e seus respectivos componentes de Backup incluindo capacidades e desempenho;

1.5.18 Cópia de dados para fins de backup, migração e restauração de grandes volumes de dados quando de necessidades específicas da CONTRATANTE, utilizando preferencialmente as ferramentas nativas dos equipamentos quando possível e/ou ferramentas agnósticas;

1.5.19 Relatórios de Health-check especializado em prevenção e correção de problemas em sistemas e equipamentos de backup, com emissão de relatórios e plano de ação preventivo ou corretivo;

1.5.20 Elaborar e executar plano de Recuperação de Desastre para validação de processos de contingência;

1.5.21 Execução de atividades de recuperação do ambiente produtivo a partir dos dados armazenados no ambiente seguro de réplica em caso de incidente cibernético;

1.5.22 Elaboração de procedimentos (scripts) de autosserviço para equipes internas de infraestrutura;

1.5.23 Emissão de relatório com os critérios de gestão de indicadores TIC, de modo a comprovar a eficácia do serviço referente ao ambiente de backup e os seus respectivos componentes, incluindo resumo executivo, capacidades, tendências e desempenho;

1.5.24 O profissional designado pela CONTRATADA deverá possuir acesso irrestrito ao serviço de suporte da fabricante DELL/EMC para abertura e consultas de chamados, à base de conhecimento, bem como contato direto com as áreas de engenharia e desenvolvimento dos produtos DELL EMC;

1.5.25 O recurso designado pela contratada deverá atuar em parceria com as demais equipes especializadas de TI da CONTRATANTE, com o intuito de solucionar os incidentes que envolvam mais de uma área de TI;

1.5.26 É de total responsabilidade da CONTRATANTE manter o profissional designado atualizado e devidamente certificado em relação a novas tecnologias e versões de produtos DELL EMC pertencentes ao ambiente de backup da CONTRATADA.

1.5.27 **Requisitos de Garantia Técnica:**

1.5.20.1 A garantia será de 60 (sessenta) meses, a partir da emissão do Termo de Recebimento Definitivo (TRD);

1.5.20.2 A garantia técnica e a manutenção do equipamento devem cobrir defeitos em quaisquer dos componentes físicos dos equipamentos fornecidos, incluindo a substituição completa ou parcial de equipamentos que venham a apresentar problemas de funcionamento, sem ônus adicional para o CONTRATANTE;

1.5.20.3 A garantia técnica e a manutenção dos equipamentos devem cobrir, também, o direito do CONTRATANTE ao recebimento de todas as novas versões ou releases dos softwares adquiridos, bem como de produtos que eventualmente venham a ser substituídos.

1.5.20.4 A garantia e assistência técnica devem englobar todos os equipamentos, seus componentes e softwares;

1.5.20.5 Os serviços referentes à garantia técnica e a manutenção dos equipamentos, e respectivos serviços de suporte técnico, devem ser prestados na modalidade on-site (presencial), em regime de 24x7 (24 horas por dia, 7 dias da semana);

1.5.20.6 As manutenções que exijam paralisação do ambiente, ou que coloquem em risco sua disponibilidade, devem ser executados fora do horário de expediente da Contratante (antes das 6:00h ou após as 22:00h em dias úteis, ou em finais de semana e feriados);

1.5.20.7 A solução ofertada deve ter prazo de garantia de funcionamento e de direito a atualização contados a partir da data da emissão do Termo de Recebimento Definitivo pelo CONTRATANTE para os dois itens.

1.5.20.8 Os custos relativos ao fornecimento da garantia devem ser computados no preço dos próprios itens referentes ao hardware e software.

1.5.20.9 Durante o prazo de garantia, a CONTRATADA deverá providenciar, sem ônus adicional para a ANEEL, o fornecimento de atualização de versão e/ou release, bem como patches de todos os softwares que integram a solução, incluindo drivers e todos os demais elementos integrantes da solução fornecida.

1.5.27.1 A garantia consiste, entre outros, em:

1.5.20.1 Reparar eventuais falhas de funcionamento, mediante a substituição de versão, de acordo com os manuais e normas técnicas específicas.

1.5.20.2 Substituir peças com defeito por outras de configuração idêntica ou superior, originais e novas, sem que isso implique acréscimo aos preços contratados;

1.5.20.3 Dispor de estoque de peças de reposição, visando à prestação dos serviços de suporte e garantia no prazo e condições estabelecidos neste Termo de Referência.

1.5.20.4 Efetuar, sem que isso implique acréscimo aos preços contratados, a substituição de qualquer equipamento, componente ou periférico por outro novo, de primeiro uso, com características idênticas ou superiores, independente do fato de ser ou não fabricante dos equipamentos fornecidos.

1.5.20.5 Responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas;

1.5.20.6 Comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os equipamentos objeto deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção;

1.5.20.7 A CONTRATADA deverá disponibilizar a atualização dos produtos licenciados assim que houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos.

1.5.20.8 O direito de atualização de versão de cada programa deverá abranger:

1.5.20.8.1 Downloads de drivers, firmwares, patches, atualizações dos softwares e manuais técnicos, a partir do sítio internet do fabricante do produto.

1.5.20.8.2 Todas as atualizações, novas versões e releases dos softwares que fizerem parte da solução contratada.

1.5.20.8.3 Direito de acesso pelos técnicos da ANEEL à base de conhecimento e a fóruns da solução no sítio do fabricante.

1.5.20.8.4 Notificar a ANEEL em prazo não superior a dez dias sobre a disponibilidade de novas versões e releases dos softwares que fizerem parte da solução fornecida.

1.5.20.8.5 Juntamente com a documentação de instalação e configuração da solução, como requisito para emissão do Termo de Recebimento Definitivo, a CONTRATADA deverá entregar a seguinte documentação:

1.5.20.8.5.1 Certificado (s) de Garantia ou outro (s) documento (s) comprobatório (s), comprovando que os softwares e equipamentos que compõe a solução estão cobertos pela garantia do fabricante, pelo prazo mínimo de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo emitido pela ANEEL.

1.5.20.8.5.2 Termo de cessões de direito ou outro (s) documento (s) comprobatório (s) garantindo o uso perpétuo dos softwares fornecidos. Os termos de licenciamento de todos os softwares fornecidos, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e os mesmos serão direito pertencentes a ANEEL.

1.5.20.8.5.3 A CONTRATADA deverá orientar a CONTRATANTE para, quando for conveniente à CONTRATANTE, proceder à aplicação de pacotes de correção e implantação de versões do produto, cabendo à CONTRATADA orientar e disponibilizar um técnico para contato, em caso de dúvidas ou falhas, por meio telefônico ou correio eletrônico.

1.5.20.8.5.4 A CONTRATADA deverá promover o isolamento, identificação e caracterização de falhas de laboratório (bugs), encaminhamento da falha ao laboratório do fabricante e acompanhamento de sua solução.

1.5.20.8.5.5 Serão consideradas falhas de laboratórios o comportamento ou características dos softwares que se mostrem diferentes daqueles previstos na documentação do produto e sejam considerados pela CONTRATANTE como prejudiciais ao seu uso.

1.5.28 Requisitos de Suporte Técnico da Garantia

1.5.21.1 Realizar atendimentos “on-site” (Severidade 1 e 2) e remotos (Severidade 3 e 4) conforme categorização dos chamados definida abaixo:

SEVERIDADE	DESCRIÇÃO	TEMPO TOTAL DE SOLUÇÃO (DEFINITIVA/CONTORNO)
1 – Urgente (alta)	Indisponibilidade total dos equipamentos ou serviço.	06 (seis) horas
2 - Muito importante (Média/alta)	Erros ou problemas que impactem o ambiente de produção.	08 (oito) horas
3 – Importante (baixa)	Problemas contornáveis que não degradam o ambiente de produção.	48 (quarenta e oito) horas
4 – Informação	Consulta técnica, dúvidas em geral, monitoramento, atualizações de software, dentre outros.	72 (setenta e duas) horas

1.5.21.2 O atendimento deverá ser categorizado em quatro níveis. A contratada deverá garantir tempo máximo de atendimento e restauração de serviço, conforme a tabela acima.

1.5.21.3 O CONTRATANTE fará a “abertura de chamados” técnicos através de ligação telefônica ou via web, em período integral 24 (vinte e quatro) horas por dia 07 (sete) dias por semana. A CONTRATADA deverá informar o número do telefone em sua proposta. Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

1.5.21.4 A CONTRATADA deverá disponibilizar suporte técnico de toda a solução, através da forma de atendimento remoto, em período integral – 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, pelo período de garantia da solução.

1.5.21.5 Na abertura do chamado, a Contratada deverá informar o número da ordem de serviço, conforme modelo a ser definido no TR;

1.5.21.6 A CONTRATADA deverá substituir peças com defeito gastas pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas, sem que isso implique acréscimo aos preços contratados.

1.5.21.7 A CONTRATADA deverá enviar mensalmente um relatório consolidado das ordens de serviço geradas no mês, mencionando data e hora de abertura do chamado técnico, número do chamado técnico, os problemas verificados, as recomendações e orientações técnicas.

1.5.21.8 A CONTRATADA deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações.

1.5.21.9 A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da ANEEL, em relação à instalação, configuração e problemas detectados, conforme prazos contidos na tabela de severidade informada anteriormente.

2. ANÁLISE COMPARATIVA DAS SOLUÇÕES EXISTENTES

2.1.1 A seguir serão descritas as soluções identificadas para a criação de um ambiente de contingência de backup (réplica) para a ANEEL.

Solução 1 – Contratação de serviços de serviços de nuvem computacional para recebimento dos dados replicados do ambiente de backup primário da ANEEL.

2.1.2 O Gartner, por meio da publicação intitulada de "Evite desastres de ransomware com uma estratégia melhor de backup e recuperação" (https://www.gartner.com/doc/reprints?id=1-

1YJl6RJ2&ct=200303&st=sb) descreve uma estratégia completa de backup e recuperação de dados e sistemas em caso de um ataque cibernético destrutivo causado por ransomwares.

2.1.3 Nesse documento, destacam-se as seguintes características técnicas que deverão ser alcançadas por uma solução de backup para prover uma proteção adequada contra ransomwares:

I. Promover o "Air-Gap" com mídia removível ou desconexão de rede: reduz a acessibilidade do malware para atacar o armazenamento de backup;

II. Utilização de appliance de backup: reduz a exposição a ataques com arquitetura reforçada e estratégia consistente de atualização/patch dos componentes.

III. Prover imutabilidade de dados utilizando WORM (Write Once, Read Many): bloqueia alterações nos dados de backup usando tecnologia específica de imutabilidade para restringir quaisquer alterações;

IV. Prover detecção durante o processo de backup: identificar anomalias rapidamente utilizando métodos de IA/ML e alertar os administradores;

V. Prover recuperação baseada em análise de ransomware: melhora a velocidade de recuperação usando detecção e análise para identificar rapidamente os dados afetados e associá-los ao melhor ponto de recuperação.

2.1.4 Baseando-se nesse documento, buscou-se inicialmente verificar a possibilidade da utilização de uma solução de computação em nuvem para atender os requisitos de segurança necessários ao provimento de ambiente de contingência de backup protegido contra ransomwares em questão.

2.1.5 Ao adotar uma solução de computação em nuvem geram-se incertezas quanto ao pleno atendimento dos requisitos em análise. Por exemplo, sabe-se que são características da computação em nuvem a realização do compartilhamento de infraestrutura de TI entre diversos locatários e a existência de conexão do ambiente computacional da nuvem com a Internet. Tais características introduzem vulnerabilidades ao ambiente em questão, sendo que essa última,

em especial, introduz riscos de segurança relativos à exposição dos dados na Internet, que poderiam resultar no acesso indevido dos dados da ANEEL por hackers ou agentes mal-intencionados para realização do vazamento ao mesmo tempo em que contaminam os dados por ransomwares, caso não estejam armazenados de forma verdadeiramente imutáveis prometidas pelo fornecedor do serviço (https://www.cisoadvisor.com.br/ataques-de-ransomware-usam-backups-na-nuvem-contra-empresas/).

2.1.6 Dessa forma, verifica-se o aumento de um risco de segurança cibernética no uso de uma solução em nuvem). Este risco, inclusive, é superior quando comparado a sua probabilidade de concretização ao se adotar uma solução de contingência “on-premise”, pois além dela permitir manter os dados isolados da rede corporativa de dados, também permite mantê-los isolados do acesso pela Internet.

2.1.7 Ressalta-se que tal risco poderá ainda ser agravado com a eventual probabilidade de vazamento de dados da Agência que estejam regulados pela Lei Geral de Proteção de Dados Pessoais (LGPD).

2.1.8 A despeito disso, mesmo que seja considerado um pleno atendimento dos requisitos de proteção por soluções de nuvem que demonstrem prover uma combinação de mecanismos de controle de acesso à infraestrutura de TI, ainda haverá a necessidade da ANEEL possuir um link de Internet (WAN) com elevadas taxas de transferência para realizar a eventual recuperação dos dados para o ambiente local em caso de ataque.

2.1.9 Entende-se que tal questão é um fator limitador para o atendimento da demanda em questão, uma vez que não trará os resultados esperados de agilidade na recuperação de dados e sistemas críticos buscados pelo negócio da ANEEL que são obtidos, em contrapartida, por meio do uso de uma solução hospedada localmente cujas taxas de velocidade existentes na comunicação efetuada na rede local (LAN) são naturalmente mais elevadas.

2.1.10 Em resumo, é possível elencar as seguintes desvantagens do uso de NUVEM como estratégia para replicação de dados de backup da ANEEL em questão:

I. Impossibilidade de validar se os dados de backup gravados na cópia remota estão livres de infecção;

II. Por padrão, é considerado menos seguro que a solução hospedada localmente (on-premise) devido à dependência da Internet (sempre “online”) ou de redes não seguras, que promove muitos pontos de acesso, onde hackers podem acessar e eventualmente copiar e destruir o armazenamento da nuvem (bucket) e, até mesmo, a conta da organização na nuvem;

III. Performance de recuperação de dados limitado ao link de comunicação;

IV. Provedores de nuvem não garantem imutabilidade dos dados (WORM) para características de compliance/governança;

V. Alto custo de recuperação (custo de download dos dados da nuvem ao ambiente local);

2.1.11 Verifica-se que a solução de replicar os dados de backup da ANEEL na nuvem apresenta uma de desvantagens e que, com isso, não se mostra a mais adequada tecnicamente para o atendimento da demanda em questão.

Solução 2 – Contratação de solução de backup de marca diversa da atualmente utilizada na Agência para montagem da réplica do backup primário no datacenter da ANEEL

2.1.12 A utilização de uma solução de fabricante diverso da solução de backup atual da ANEEL com diferentes produtos para se integrar não se aplica por restrições técnicas pois, como o próprio nome diz, trata-se de um ambiente de “réplica” , ou seja, por questões de compatibilidade e interoperabilidade entre os componentes da solução, o ambiente de réplica precisa possuir as mesmas características do atual ambiente de backup primário na ANEEL, visto que as informações dos dados copiados nesta infraestrutura, assim como seus dados de controle, serão replicados/copiados de maneira idêntica, onde apenas o software e os equipamentos utilizados na gravação (origem) terão condições de ler e recuperar os dados replicados para dentro deste ambiente seguro.

2.1.13 Portanto, o uso de qualquer outra solução diversa da solução utilizada no ambiente primário de backup trará maior complexidade e risco à integridade dos dados armazenados nesse ambiente, podendo inclusive causar a corrupção ou até mesmo perda dos dados já salvos. Além disso, por se tratar de informações de backup, há ainda um volume grande de dados legados, que não podem ser lidos ou recuperados por solução de outro fabricante.

2.1.14 Sendo assim, pelas razões acima apresentadas, a contratação de solução de backup de marca diversa da solução atual para compor o ambiente de réplica de backup da ANEEL também não se mostra a mais adequada tecnicamente para atendimento da demanda em questão.

Solução 3 – Expansão da atual solução de backup da ANEEL para montagem do ambiente de contingência (réplica de backup) no datacenter da ANEEL

2.1.15 O ambiente de **backup primário da ANEEL** é composto pela suíte de softwares de backup da marca "DELL Data Protection Suite" e pelo subsistema de armazenamento (appliance de backup) da marca "DELL EMC Data Domain DD 6800" com garantia vigente até novembro de 2022 entre outros componentes, também da fabricante DELL, tais como a biblioteca de fitas e solução de arquivamento (Processos Sicnet nº 48500.005102/2017-63 e 48500.003304/2016-90).

2.1.16 Considerando-se o uso de uma estratégia de réplica do ambiente de backup primário, os aspectos técnicos dessa solução utilizada na ANEEL foram analisados também à luz dos principais pontos técnicos contidos no artigo do Gartner citado anteriormente para fins de verificação de sua adequabilidade no atendimento da demanda em questão.

2.1.17 Em consulta à página do fabricante foi possível identificar que o referido appliance de backup da ANEEL suporta o modo de isolamento seguro ou "air-gap" de maneira nativa sem custos adicionais, modo que reduz o acesso ao equipamento por malwares em caso de ataque cibernético em questão (https://www.delltechnologies.com/pt-br/data-protection/cyber-recovery-solution.htm).

2.1.18 Verificou-se também que a solução de backup da marca “DELL Data Domain” possui recurso de imutabilidade dos dados utilizando funcionalidades de WORM (Write Once Read Many) que garante que o dado salvo não poderá ser alterado ou apagado por malwares destrutivos. Destaca-se que tal recurso já foi implementado pela equipe técnica da ANEEL para um dos sistemas críticos (SICNET2) no appliance de **backup primário da Agência** e que, deverá ser aplicada também nos dados armazenados no equipamento de réplica garantindo-se dessa forma que a proteção contra tais ataques seja abrangente, sobretudo para os dados críticos armazenados no ambiente de contingência.

2.1.19 Quanto ao provimento de detecção de ataques ransomwares, em consulta ao sítio do fabricante “Dell EMC” verificou-se que o módulo “CyberSense” contido na suíte completa “Data Protection Suite” é capaz de realizar a análise, relatório e automatização de todo processo de validação em relação a integridade dos dados salvos, atendendo as necessidades relacionadas à detecção, análise, relatório e recuperação diante de ataques cibernéticos destrutivos (https://www.dellemc.com/pt-br/collaterals/unauth/briefs-handouts/solutions/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf).

2.1.20 Tal módulo funciona de forma integrada com o software de backup “Dell EMC Networker” do “Dell Data Protection Suite” em uso na ANEEL, permitindo que todas as cópias de backup realizadas e replicadas sejam verificadas através de métodos de inteligência artificial (IA) para garantir que as informações salvas estão livres de contaminação por algum tipo de ransomware.

2.1.21 Por meio de consulta ao sítio do fabricante foi possível constatar ainda que o software de backup “Dell EMC Networker”, em uso pela ANEEL, é avaliado como líder no quadrante mágico pelo Gartner há pelo menos 20 anos (https://blog.dellemc.com/en-us/dell-emc-data-protection-two-decades-of-leadership-gartner-magic-quadrant/).

2.1.22 Sobre padrões internacionais, verifica-se que a fabricante da solução de backup atual da ANEEL atende às demandas técnicas recomendadas pelas melhores práticas internacionais

estabelecidas para continuidade de negócios em decorrência de ataques cibernéticos. Nesse requisito exemplifica-se que a solução é recomendada pelo grupo internacional Sheltered Harbor (https://shelteredharbor.org/), caracterizada por ser uma iniciativa norte-americana sem fins lucrativos, que compreende instituições financeiras, provedores de serviços básicos, associações comerciais nacionais, parceiros de aliança e provedores de soluções dedicados a aumentar a estabilidade e resiliência do setor financeiro contra ataques cibernéticos.

2.1.23 Nesse aspecto, verificou-se que a Dell é listada como fabricante homologado por esse grupo internacional, conforme citado em https://blog.dellemc.com/en-us/dell-technologies-joins-sheltered-harbor-alliance-partner-program-as-first-solution-provider/ para fornecimento de solução de contingência e recuperação de ataques cibernéticos destrutivos, por meio da adoção da arquitetura cujo cerne é a criação de um "Data Vault" para proteção definitiva dos dados contra infecção por ransomwares e wipers.

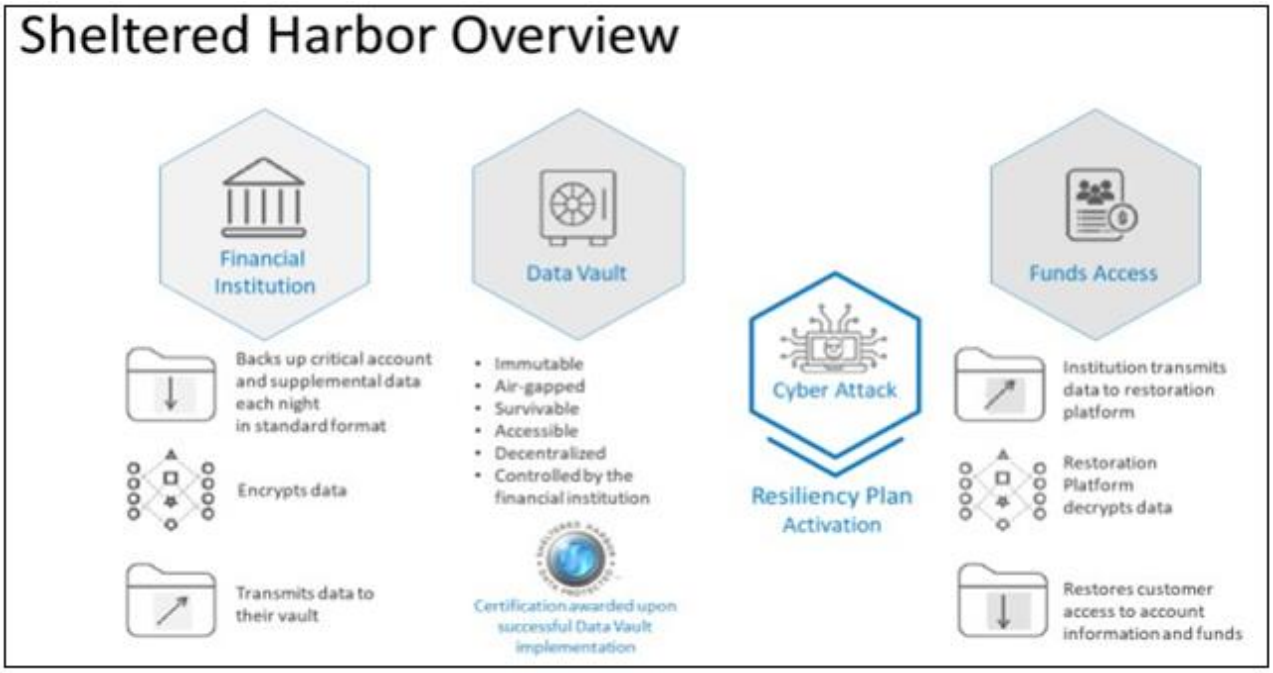

Figura 1 *– "Data Vault": arquitetura de backup seguro com dados imutáveis (immutable) e isolados da rede corporativa (air-gapped) (fonte: https://shelteredharbor.org/how-it-works)*

2.1.24 Esta arquitetura compreende, de forma sintética, a realização da réplica dos dados de backup primário da organização para um ambiente secundário (Data Vault), isolado da rede corporativa (air-gapped), contendo requisitos de segurança cibernética adicionais destinados à proteção e restauração de dados de sistemas críticos de organizações financeiras em caso de ataques cibernéticos destrutivos (imutabilidade dos dados, análise de malwares realizados nos dados de backup replicados e ambiente de servidores virtuais de recuperação também segmentados da rede corporativa).

2.1.25 Nesse sentido, a DELL propõe uma solução de "*Data Vault*" para proteção, backup e recuperação de dados e sistemas críticos contra ataques cibernéticos destrutivos por meio da seguinte arquitetura (destaque circundado em amarelo – *Cyber Recovery Vault*).

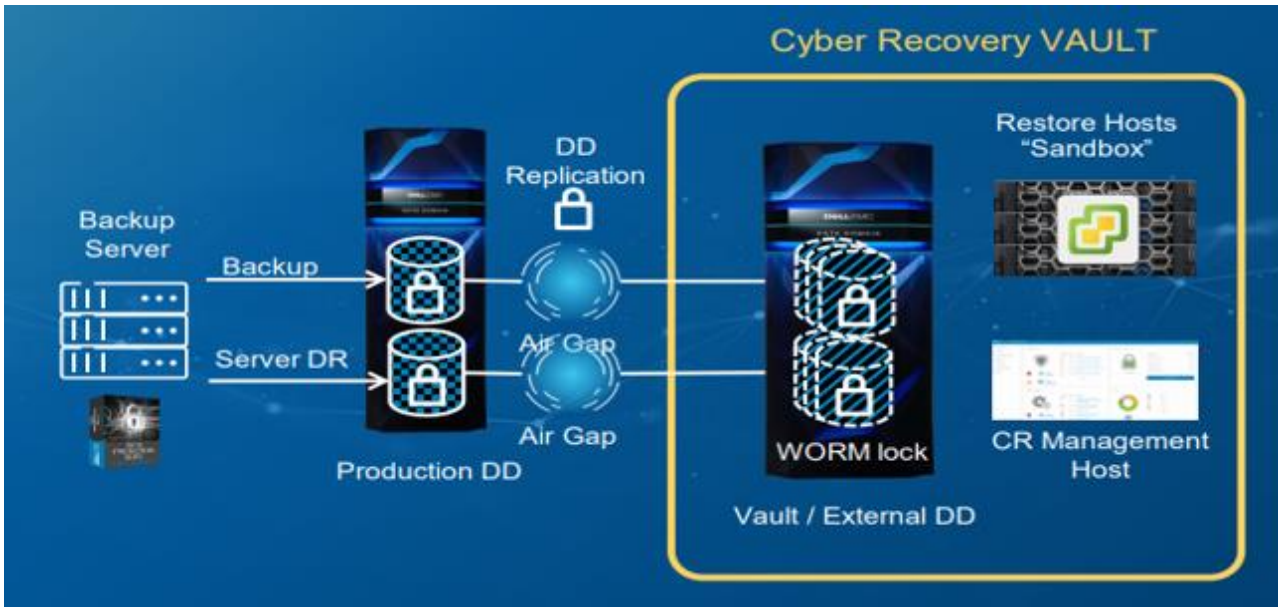

Figura 2 *– Arquitetura denominada "Cyber Recovery Vault" definida pela DELL para implementação do padrão de proteção de dados contra ataques cibernéticos destrutivos (Data Vault) promovida pela organização internacional "Sheltered Arbor"*

2.1.26 Sendo assim, considerando que a ANEEL já possui a infraestrutura denominada "*Production DD*" (Data Domain 6800) da figura acima, a criação de um ambiente de contingência e recuperação de backup dotado das características citadas anteriormente (Cyber Recovery Vault), utilizando-

se, portanto, de uma réplica da solução de backup atual da ANEEL (DELL Data Domain 6800) e adicionando as funcionalidades de segurança contra ataques de ransomwares, à solução é, do ponto de vista técnico, a que melhor proverá o atendimento efetivo da demanda de proteção isolada, detecção de malwares e recuperação acelerada de dados e sistemas críticos da ANEEL contra ataques cibernéticos destrutivos.

2.1.27 Portanto, constatou-se pelo presente estudo que a criação de um ambiente de réplica de backup utilizando componentes de hardware e software de mesmo fabricante da atual solução de backup da ANEEL, trará as seguintes vantagens do ponto de vista técnico à ANEEL em comparação às outras soluções analisadas:

I. Menores riscos operacionais relativos à disponibilidade e estabilidade do datacenter e relativos à integridade dos dados de aplicações da ANEEL armazenadas no ambiente de backup primário por meio da construção de um ambiente de réplica de backup com total compatibilidade e integração com a atual solução de backup da Agência;

II. Maior velocidade na recuperação de sistemas de informação críticos diante de um ataque cibernético destrutivo, uma vez que os dados críticos dessas aplicações estarão replicados numa infraestrutura de backup local totalmente compatível e integrada à infraestrutura de backup primário da Agência;

III. Melhor gerenciamento dos equipamentos que compõem a solução como um todo (ambiente primário + ambiente de réplica) devido à compatibilidade integral com a solução de hardware e software de backup primário;

IV. Garantia de imutabilidade dos dados críticos de backup replicados do ambiente de backup primário contra a alteração (criptografia) ou eliminação não autorizada (wipers), por meio do uso de software avançado de detecção e análise de malware (Cybersense),

seguindo as melhores práticas internacionais de proteção de dados, continuidade de negócios e recuperação contra ataques cibernéticos destrutivos;

V. Diminuição significativa dos impactos de ataque de ransomware por meio da detecção acelerada de sua presença no ambiente de backup primário, ao se utilizar software avançado de detecção e análise de malwares que emprega técnicas de inteligência artificial e machine learning logo após a replicação dos dados de backup no ambiente de contingência (Cybersense).

VI. Melhor retorno de investimento e custo de manutenção realizado ao longo dos anos pela Agência na solução de backup atual (hardware e software) e em capacitações de recursos humanos internos;

2.1.28 Quanto ao atendimento dos seguintes requisitos, verifica-se que a solução 3:

Requisito	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	X		
A Solução está disponível no Portal do Software Público Brasileiro?		X	
A Solução é um software livre ou software público?		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	X		
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do – e-ARQ Brasil? (Quando o objetivo da solução abranger documentos arquivísticos)			X

3. ANÁLISE COMPARATIVA DAS SOLUÇÕES VIÁVEIS EM TERMOS DE CUSTOS

3.1 Conforme análise realizada na seção 2 anterior, foi verificado que a única solução viável e funcional que atende com segurança todos os requisitos técnicos da demanda é a realização da expansão da

atual solução de backup da ANEEL para a montagem do ambiente de contingência (réplica) local visando salvaguardar os dados dos sistemas críticos da ANEEL contra ataques de ransomwares.

3.2 Para tanto, foi solicitado ao fabricante Dell a obtenção da estimativa de espaço de armazenamento para o appliance de backup da réplica com vistas ao atendimento desse projeto. Com base na capacidade do storage da ANEEL (200 TB) o fabricante estimou em 120 TB (cento e vinte terabytes) o espaço necessário para acomodar um volume inicial dos dados de sistemas críticos. Os emails contendo as informações eletrônicas sobre a capacidade estimativa realizada pelo fabricante estão disponíveis no referido ANEXO I – Capacidade estimada pelo fabricante.

3.3 Com base nessa estimativa, os seguintes componentes tecnológicos da solução que comporão o ambiente de réplica de backup da ANEEL e os serviços necessários da contratação foram consolidados na tabela a seguir:

	Itens (hardwares, softwares e serviços) necessários para compor o ambiente de contingência (réplica de backup)		
Item	**Descrição**	**Unidade**	**Quantidade**
1	Appliance de backup “DELL Data Domain”	Equipamento	1
2	Módulo de expansão de capacidade do appliance de backup “DELL Data Domain”	Equipamento	2
3	Expansão do software de backup “DELL Data Protection Suite”	Processador	8
4	Expansão do módulo “Cybersense Data Protection Suite “	Terabyte (TB)	120
5	Expansão do software ”VMWare NSX”	Processador	8
6	Switch de comunicação de rede LAN	Equipamento	2
7	Serviços de implementação da solução	Serviço	1
8	Serviços especializados de suporte	horas	300

3.4 As justificativas e quantitativos de cada um dos itens da tabela acima foram detalhados a seguir:

3.4.1 **Appliance de backup “DELL Data Domain”:** Será adquirido um novo hardware de backup “Dell Data Domain”, que atuará como réplica do atual equipamento de backup prinário da ANEEL (Dell Data Domain 6800), com garantia de atualização e suporte técnico por 60 (sessenta) meses, destinado

à realização do armazenamento imutável dos dados replicados e por mantê-los isolados da rede corporativa da ANEEL (air-gapped), com capacidade mínima de 120 TB úteis e que representa, inicialmente, 60% (sessenta por cento) da capacidade da solução de storage da ANEEL com garantia e suporte técnico do fabricante por 60 meses.

3.4.2 **Módulo de expansão de capacidade do appliance de backup "DELL Data Domain":** Visto que poderão ser adicionados novos sistemas críticos e atualizada a política de backup conforme as necessidades da ANEEL, e que isto poderá resultar em aumento da necessidade de espaço de armazenamento no appliance de backup adquirido no item 1, se faz prudente incluir uma previsão de expansão de sua capacidade em até 80 (oitenta) TB úteis além dos 120 TB úteis previstos no item 1, com garantia e suporte técnico do fabricante por 60 (sessenta) meses. Com isso, será possível chegar ao total armazenado de 200 (duzentos) TB úteis que representa a totalidade da capacidade da solução de storage da ANEEL durante o prazo de vigência da ata de registro de preços desta contratação, para acompanhar a expansão de necessidades de armazenamento adequando-se os prazos de retenção de dados de sistemas críticos.

3.4.3 **Expansão do software de backup "DELL Data Protection Suite":** Será expandido o atual licenciamento perpétuo por processadores do software de backup da ANEEL "Networker" contido no "Dell Data Protection Suite" para 8 (oito) processadores, com garantia de atualização e suporte por 60 (sessenta) meses, visando contemplar a realização de backup dos 4 (quatro) novos servidores físicos de hiperconvergência, cada um contendo 2 (dois) processadores físicos, recém-adquiridos em outra contratação da ANEEL e que comporão o ambiente de réplica, para fins de hospedagem do software de backup e de possibilitar a recuperação dos sistemas e dados em ambiente isolado antes de transferência à produção.

3.4.4 **Expansão do módulo "Cybersense Data Protection Suite**": Será expandido a licença de software perpétuo do software de backup "Dell Data Protection Suite" para conter o módulo de software denominado "Cybersense", licenciado por por Terabytes (TB) que realizará a detecção,

análise e alerta da presença de malwares destrutivos nos dados de backup replicados, para um volume de 120 TB úteis, com garantia de atualização e suporte técnico por 60 (sessenta) meses. Não se verifica a necessidade de expansão deste item junto com item 2 uma vez que a expansão dele será utilizada para aumentar o volume armazenado no appliance e com isso, a quantidade e o prazo de retenção de cópias, que já terão sido em grande parte analisada pelo cybersense na cópia inicial.

3.4.5 **Expansão do software ”VMWare NSX”:** Será expandido o licenciamento perpétuo do software de microssegmentação de redes (VMware NSX), licenciado atualmente por processadores na ANEEL, com garantia de atualização e suporte técnico por 60 (sessenta) meses, necessário para garantir o isolamento (firewall virtual) da rede corporativa da ANEEL dos 4 (quatro) servidores físicos da solução, cada um contendo 2 (dois) processadores físicos, recém-adquiridos em outra contratação da ANEEL e que comporão o ambiente de contingência;

3.4.6 **Switch de comunicação de rede LAN:** Será adquirido 2 (dois) switches de rede local que permitirão a conectividade de dados, em alta-disponibilidade, dos equipamentos do ambiente de contingência, com garantia de atualização e suporte técnico por 60 (sessenta) meses.

3.4.7 **Serviços de implementação da solução:** Será contratado o serviço de instalação e configuração da solução no datacenter da ANEEL para os equipamentos e softwares contidos nos itens anteriores;

3.4.8 **Serviços especializados de suporte:** Será contratado o serviço adicional de suporte especializado do fabricante pois, ao se adicionar um nova solução à diversidade de soluções já em uso no datacenter da ANEEL, aumenta-se a complexidade técnica da operação e administração do ambiente de TI que exige um nível cada vez maior de conhecimento, levando-se a um degrau de esforço no sentido de torná-lo mais estável, seguro e sempre disponível para os usuários internos e externos a ANEEL. Por esse motivo, identificou-se a necessidade de complementar essa contratação para incluir os serviços especializados de operação assistida direto do fabricante, cujos trabalhos irão apoiar a equipe de TI da ANEEL de forma direta, com emprego das melhores práticas de mercado,

definição de arquitetura, resolução de problemas em caso de incidente, acesso direto ao suporte e material da engenharia do produto, garantindo o pleno funcionamento e disponibilidade deste ambiente. O quantitativo de 300 (trezentas) horas poderão ser utilizados na medida das necessidades de serviços com conhecimentos especializados, como por exemplo, configurações de políticas de backup de sistemas críticos, testes de recuperação de dados em backup e eventual necessidade de acionamento em decorrência de necessidade real de recuperação de dados em caso de ataque cibernético de ransomware.

3.5 Estimativa de custos totais da contratação

3.5.1 Para obtenção da estimativa de custo e preços de referência para a contatação, foi realizada inicialmente uma pesquisa de preços utilizando o painel de preços do governo federal.

3.5.2 Para tanto, foram realizadas buscas no referido portal, tanto em “Materiais” quanto em “Serviços” pelas expressões “backup”, “cópias de segurança”, “switch”, “vmware” e “virtualização” no campo “objeto da compra” e escolhida as contratações ocorridas no período de 1(um) ano anteriores à data de elaboração deste documento.

3.5.3 Nessas buscas foram encontrados alguns processos de contratação que, após a análise quanto à similaridade com os itens do objeto da contratação em tela, foram selecionados e incluídos com os respectivos preços dos itens contratados na tabela 1 a seguir (no ANEXO I – Pesquisa de preços e mercado - estão contidos documentos das contratações obtidas):

Tabela 1 - Pesquisa de Preços - Réplica de Backup (Preços obtidos do Painel de Preços do Governo Federal)

Pregão	Descrição	Valor unitário no painel de preços (vigência original da contratação)	Valor unitário mensal calculado
Item 1 - Appliance de backup			
PE 007/2019 - Universidade Federal do Pará (UFPA) - Contratação de empresa	Item 5 - Sistema de armazenamento de backup (appliance de backup) por 60	R$ 410.000,00 por 3 anos (1 appliance)	R$ 11.388,88 por appliance (V1)

	especializada no fornecimento de soluções de Armazenamento e Backup de Dados (equipamentos e softwares), inclusos os serviços de instalação, configuração, garantia e suporte técnico	meses (Eqto. Entregue DELL Data Domain 6300)			
	PE 18/2020 - TCDF - Contratação de empresa especializada para fornecimento de solução de proteção de dados, compostas por... appliance de backup...com suporte e garantia on site por 60 meses	ITEM 1: Solução de proteção de dados, composta por 1 (um) software e 2 (dois) appliances de backup, com garantia on site por um período de 60 meses (Eqto. Entregue DELL Data Domain 6300)	R$ 699.245,50 por 5 anos (1 appliance)	R$ 11.654,09 por appliance (V2)	
	PE 32/2019 - ANAC - Aquisição de Solução de Cópia de Segurança (Backup), incluindo licenças perpétuas de Software de Gerenciamento de Backup, Subsistema Inteligente de Backup em Disco com desduplicação, treinamento, serviços de instalação, configuração, suporte técnico e garantia por 60 meses.	ITEM 1: Subsistema Inteligente de Backup em Disco com 250 TB de espaço sem considerar taxa de desduplicação e compactação e com Suporte e Garantia de 60 meses. (Entregue Veritas NetBackup 5240) - Desconsiderado em virtude da solução ser de marca diversa do equipamento objeto deste item da contratação	R$ 625.000,00 por 5 anos (1 appliance) (desconsiderado)	R$ 10.416,67 por appliance (desconsiderado) (V3)	
	Valor unitário médio mensal (V1+V2) /2 (Vapp)		R$ 11.521,49		
	Valor total estimado para 60 meses (Vapp*60)		R$ 691.289,10		
	Item 2 - Expansão de appliance de backup				
	PE 007/2019 - Universidade Federal do Pará (UFPA) - Contratação de empresa especializada no fornecimento de soluções de Armazenamento e Backup de Dados (equipamentos e softwares), inclusos os serviços de instalação, configuração, garantia e suporte técnico, operação	Item 6 - Módulo de expansão de appliance de backup com capacidade mínima de 45 TB (Dell Data Domain modules)	R$ 265.000,00 por 3 anos (1 módulo)	R$ 7.361,11 por módulo	

	assistida e transferência de conhecimento			
	Valor unitário médio mensal		R$ 7.361,11	
	Valor total estimado para 60 meses (1 módulo)		R$ 441.666,10	
	Valor total estimado para 60 meses (2 módulos)		R$ 883.332,20	
	Item 3 - Expansão do Software de backup			
	PE 007/2019 - Universidade Federal do Pará (UFPA) - Contratação de empresa especializada no fornecimento de soluções de Armazenamento e Backup de Dados... inclusos os serviços de instalação, configuração, garantia e suporte técnico por 60 meses	Item 8 - Software para cópias de segurança (software de backup) por processador (software DELL Networker)	R$ 19.000,00 por processador (5 anos)	R$ 316,67/mês (por processador) (V4)
	PE 32/2019 - ANAC - Aquisição de Solução de Cópia de Segurança (Backup), incluindo licenças perpétuas de Software de Gerenciamento de Backup, Subsistema Inteligente de Backup em Disco com desduplicação, treinamento, serviços de instalação, configuração, suporte técnico e garantia por 60 meses.	Item 1 - Software de Gerenciamento de Backup com Suporte e Garantia de 60 meses (software VERITAS NETBACKUP) Desconsiderado em virtude da solução ser de marca diversa do software objeto deste item da contratação	R$ 5.000,00 por processador (5 anos)	R$ 83,33/mês (por processador) (V5)
	Valor unitário médio mensal (V4)(por processador ao mês)		R$ 316,67	
	Valor total estimado para 60 meses (1 processador)		R$ 19.000,20	
	Valor total estimado para 60 meses (8 processadores)		R$ 152.001,06	
	Item 4 - Expansão módulo Cybersense Data Protection Suite			
	(Não foi possível obter contratações para este item no painel de preços em função de suas peculiaridades)			
	Valor unitário médio mensal		R$ 0,00	
	Valor médio para 60 meses		R$ 0,00	
	Item 5 - Expansão do software VMWare NSX			
	PE 53/2019 - CNJ - Aquisição de softwares de virtualização VmWare, incluindo serviços de desing, planejamento, customização,	Item 3 - Grupo 1 -Suite de licenças de software de virtualização de rede e segurança VmWare NSX EnterprisePlus com subscrição e suporte pelo	R$ 43.886,26 por processador (3 anos)	R$ 1.219,06/mês por processador (V7)

	implementação e treinamento oficial	período de 3 (três) anos para 32 processadores		
	PE 79/2019 - BRB - licenciamento VmWare, com prazo de suporte por 36 meses, e contratação de créditos de serviço especializado do fabricante	Item 2 - Licenças VmWare NSX advanced 6 com 3 anos de subscrição	R$ 67.878,7 por processador (3 anos)	R$ 1.885,50/mês por processador (V8)
	Valor unitário médio mensal (V7+V8)/2		R$ 1.552,28	
	Valor total para 60 meses (1 processador)		R$ 93.136,80	
	Valor total para 60 meses (8 processadores)		R$ 745.094,40	
	Item 6 - Switch de comunicação de rede LAN			
	PE 66/2020 - GDF - Secretaria de Economia - Switches tipo Core, Spine e Leaf (ToR) rede de dados para Data Center com instalação, configuração e suporte técnico e garantia pelo prazo de 60 meses	Item 1 - Switch Leaf Tor para datacenter com instalação, garantia e suporte técnico por 60 meses	R$ 212.000,00 (5 anos)	R$ 3.533,33/mês
	Valor unitário médio mensal (1 switch)		R$ 3.533,33	
	Valor total para 60 meses (1 switches)		R$ 211.999,80	
	Valor total para 60 meses (2 switches)		R$ 423.999,60	
	Item 7 - Serviços de implementação da solução			
	PE 007/2019 - Universidade Federal do Pará (UFPA) - Contratação de empresa especializada no fornecimento de soluções .... Backup de Dados (equipamentos e softwares), inclusos os serviços de instalação, configuração, garantia e suporte técnico	Item 7 - Serviço de implementação para appliance de backup + Item 9 - Serviço de implementação para software de backup	R$ 266.000,00 por serviço (V12)	Não se aplica
	PE 53/2019 - CNJ - Aquisição de softwares de virtualização VMWare, incluindo serviços de desing, planejamento, customização, implementação e treinamento oficial	Item 4- grupo 1- Serviços de design, planejamento, customização e implementação dos itens 1, 2 e 3, de acordo com especificações do Termo de Referência.	R$ 369.639,32 por serviço (V13)	Não se aplica
	Valor total do serviço de implementação da solução (V12+V13)/2		R$ 317.819,66	

Item 8 - Serviços Especializados de Suporte			
PE 007/2019 - Universidade Federal do Pará (UFPA) - Contratação de empresa especializada no fornecimento de soluções .... Backup de Dados (equipamentos e softwares), inclusos os serviços de instalação, configuração, garantia e suporte técnico	Item 21 - Serviço de suporte especializado	R$ 203 por hora (V14)	Não se aplica
PE 79/2019 - BRB - licenciamento Vmware, com prazo de suporte por 36 meses, e contratação de créditos de serviço especializado do fabricante	item 4 -Serviços profissionais do fabricante	R$ 373,13 por hora (V15)	Não se aplica
Valor unitário médio (V14+V15)/2		R$ 288,07	
Valor total dos serviços especializados de suporte (300 horas)		R$ 86.421,00	
VALOR ESTIMADO GLOBAL (PAINEL DE PREÇOS)			
VALOR GLOBAL ESTIMADO DA CONTRATAÇÃO PELA ANEEL (1 app. de backup + 2 módulos de expansão do app. + 8 exp. soft. backup + 8 exp. cybersense* + 8 exp. nsx + serviço de instalação + 300 horas de serviços especializados)		**R$ 3.299.957,56***	
*Ao valor global ainda deverá ser adicionado o valor do "*item 4 - Software Cybersense*" que não foi possível ser obtido na pesquisa de preços de contratações públicas (painel de preços). * A ANEEL irá adquirir os quantitativos do "*item 2- Expansão Dell Data Domain"* conforme a sua necessidade durante o prazo de vigência da ATA.			

3.5.4 A tabela acima contém os preços unitários das contratações considerando os seus diferentes prazos de vigência (36 e 60 meses) e os preços unitários mensais derivados a partir desses prazos. Com isso, foi calculada a média aritmética desses preços unitários mensais e tais valores médios foram multiplicados pelos quantitativos da contratação em tela, considerando o prazo de vigência de 60 (sessenta meses) para a contratação em questão.

3.5.5 Quanto ao "*item 5 - Expansão do software Vmware NSX*", foi realizada consulta ao catálogo de soluções de TIC com condições padronizadas – VMware, disponibilizado na url

https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-produtos-e-servicos-vmware.pdf para fins de obtenção de valores para o produto NSX da Vmware. Entretanto o catálogo não prevê entre seus itens o produto em questão.

3.5.6 Ressalta-se que não foi possível encontrar preços para o "item 4 - Expansão módulo Cybersense Data Protection Suite" no painel de preços. Em função de suas peculiaridades, também não foi possível identificar softwares semelhantes que pudessem eventualmente ser utilizados como substitutos adequados para obtenção de preços no painel de preços do governo federal.

3.5.7 Observa-se também que não foi possível obter o mínimo de 3 (três) cotações de preços para cada um dos itens dessa contratação com objetos similares. Isto ocorreu devido às peculiaridades de cada contratação (especificações técnicas e níveis de serviços, por exemplo) que, quando analisadas com maior profundidade, foram descartadas quando não se mostraram semelhantes às características da contratação em questão.

3.5.8 Com isso, foi necessário complementar a pesquisa de preços no painel de preços por meio de outras fontes. Considerando que as contratações obtidas na pesquisa anterior também se repetem na pesquisa com órgãos públicos (p.ex.: portal Comprasnet) e que não foram encontradas mídias, sites especializados e sites de domínio amplo que fornecem preços para os itens em questão, partiu-se para a cotação de preços direta com fornecedores cujos resultados foram transcritos a seguir:

Tabela 2 - Componentes do ambiente de contingência (réplica de backup)

Lote	Item	Descrição	Unidade	Quantidade
1	1	Appliance de backup Dell Data Domain	Equipamento	1
	2	Módulo expansão de capacidade do equipamento DELL Data Domain	Equipamento	2
	3	Expansão do software de backup DELL Data Protection Suite	Processador	8
	4	Expansão módulo Cybersense Data Protection Suite	TB	120
	5	Expansão do software VMWare NSX	Processador	8
	6	Switch de comunicação de rede LAN	Equipamento	2

	7	Serviços de implementação da solução	Serviço	1
	8	Serviços especializados de suporte	horas	300

3.5.9 Foi encaminhado email de pesquisa de preços, conforme ANEXO III - Pesquisa de Mercado deste documento para as empresas listadas na tabela a seguir e envidados esforços de contato para obtenção de retorno das cotações junto a elas. Com isso, as empresas que responderam à pesquisa também foram destacadas na tabela a seguir:

Tabela 3 - Pesquisa de Mercado (empresas encaminhadas e status da resposta)	
Nome da Empresa	**Respondeu à pesquisa (Sim/Não)**
BRISA Soluções em TI	**Sim**
PERFILCOMP Informática	**Sim**
CPD Informática	**Não**
SYSTECH Tecnologia da Informação	**Sim**
PPN Tecnologia da Informação	**Não**
SYNNEX Westcom	**Não**
LTA RH Infomática	**Não**

3.5.10 A pesquisa de mercado com as cotações recebidas das 3 (três) empresas acima listadas foi consolidada na tabela a seguir:

Tabela 4 - Pesquisa de Mercado - Réplica de backup (Preços obtidos diretamente com fornecedores da solução)

Descrição	Und.	Qtd.	Valor Unitário (R$)			Valor Unitário Médio (R$)	Menor Valor Unitário (R$)	Valor Total (R$)			Valor Total Médio (R$)	Menor Valor Total (R$)
			PERFIL	SYSTECH	BRISA			PERFIL	SYSTECH	BRISA		
Appliance de backup Dell Data Domain com garantia e suporte por 60 meses	Eqto.	1	2.150.550,00	2.146.750,48	2.152.285,98	2.149.862,15	**2.146.750,48**	2.150.550,00	2.146.750,48	2.152.285,98	**2.149.054,21**	**2.146.750,48**
Módulo expansão de capacidade do equipamento Dell Data Domain com garantia e suporte por 60 meses	Eqto.	2	693.150,00	660.269,18	668.649,10	**674.022,76**	**660.269,18**	1.386.300,00	1.320.538,36	1.337.298,21	**1.348.045,52**	**1.320.538,36**
Expansão do software de backup Dell Data Protection Suite	Processador	8	23.470,00	26.672,43	26.347,71	**25.496,71**	**23.470,00**	187.760,00	213.379,49	210.781,70	**203.973,73**	**187.760,00**

com garantia e suporte por 60 meses												
Expansão módulo Cybersense Data Protection Suite com garantia e suporte por 60 meses	TB	120	12.880,00	14.236,03	14.695,33	**13.937,12**	**12.880,00**	1.545.600,00	1.708.323,38	1.763.439,36	**1.672.454,25**	**1.545.600,00**
Expansão do software VMWare NSX com garantia e suporte por 60 meses	Processador	8	51.810,00	105.615,42	104.329,67	**104.972,54**	**51.810,00**	414.480,00	844.923,37	834.637,34	**839.780,36**	**414.480,00**
Switch de comunicação de rede LAN com garantia e suporte por 60 meses	Eqto.	2	224.050,00	242.957,745	256.000,00	**241.002,58**	**224.050,00**	448.100,00	485.915,49	512.000,00	**482.005,16**	**448.100,00**
Serviços de implementação da solução	Serviço	1	328.125,00	404.929,58	350.000,00	**361.018,19**	**328.125,00**	328.125,00	404.929,58	350.000,00	**361.018,19**	**328.125,00**
Serviços especializados de suporte	Horas	300	1.050,00	1.052,81	980,00	**1.027,60**	**980,00**	315.000,00	315.845,07	294.000,00	**308.281,69**	**294.000,00**
Valor Global da Contratação (R$)								6.775.915,00 (Perfil)	7.440.605,22 (Systech)	7.454.442,59 (Brisa)	**7.223.654,27 (Valor Global dos Preços Médios) (A)**	**6.685.353,84 (Valor Global dos Menores Preços) (B)**
Valor Global da Contratação utilizando-se das médias dos preços unitários obtidos (R$)											**7.223.654,27 (A)**	
Valor Global da Contratação utilizando-se dos menores preços unitários obtidos (R$)											**6.685.353,84 (B)**	

3.5.11 Nesta pesquisa com fornecedores foram obtidos dois valores para fins de comparação: o valor global dos preços unitários médios das 3 (três) propostas de mercado encaminhadas, representado por (A) na tabela acima, e o valor global dos menores preços unitários das 3(três) propostas de mercados encaminhadas, representado por (B). Como o valor representado por (B) é menor do que o valor representado por (A), optou-se pela utilização do valor representado por (B) - R$ 6.685.353,84 - que é relativo ao SOMATÓRIO DE TODOS OS MENORES VALORES DE CADA UM DOS ITENS DA CONTRATAÇÃO OBTIDOS NAS PROPOSTAS COMERCIAIS ENCAMINHADAS PELOS FORNECEDORES.

3.5.12 Observa-se que em alguns itens da tabela 4 acima há uma diferença significante de valores entre os preços obtidos no painel de preços e os preços obtidos diretamente com fornecedores. Entende-se que esta diferença se dê em virtude da variação das cotações do dólar na época da realização das contratações (maiores atualmente), uma vez que a solução é importada, à diferença dos índices

inflacionários e o cenário atual de pandemia. Além disso, destaca-se que os modelos dos equipamentos obtidos na pesquisa de painel de preços (Dell Data Domain 6300) são de uma linha inferior, não sendo mais fornecidos pela fabricante, que o substituiu por um modelo mais moderno (Dell Data Domain 6900).

3.5.13 Por fim, uma vez obtidos os preços estimados no painel de preços do Governo Federal e na consulta direta às empresas fornecedoras da solução de TI em questão, os preços finais de referência foram então consolidados na tabela a seguir:

Tabela 5 - Preços Finais de Referência para a Contratação – Réplica de Backup
(Pesquisa consolidada contendo a média dos preços obtidos dos itens no painel de preços governamentais e os menores valores das pesquisas de preços diretamente com fornecedores)

Lote	Item	Descrição	Unidade	Quantidade	Valor Unitário Médio (Painel de Preços) (R$) (X)	Menor Valor Unitário (Pesquisa de Mercado) (R$) (Y)	Valor unitário Médio das Pesquisas (R$) (X+Y)/2	Valor Total Médio (R$)
1	1	Appliance de backup Dell Data Domain com garantia e suporte por 60 meses	Equipamento	1	691.289,10	2.146.750,48	1.419.019,79	1.419.019,79
	2	Módulo expansão de capacidade do equipamento DELL Data Domain com garantia e suporte por 60 meses	Equipamento	2	441.666,10	660.269,18	550.967,64	1.101.935,28
	3	Expansão do software de backup DELL Data Protection Suite por garantia e suporte por 60 meses	Processador	8	19.000,00	23.470,00	21.235,00	169.880,00
	4	Expansão módulo Cybersense Data Protection Suite com garantia e suporte por 60 meses	TB	120	(Não foi possível obter)	1.545.600,00	1.545.600,00	1.545.600,00
	5	Expansão do software VMWare NSX com garantia e suporte por 60 meses	Processador	8	93.136,80	51.810,00	72.473,40	579.787,20
	6	Switch de comunicação de	Equipamento	2	211.999,80	224.050,00	218.024,90	436.049,80

		rede LAN com garantia e suporte por 60 meses						
	7	**Serviços de implementação da solução**	Serviço	1	**317.819,66**	**328.125,00**	**322.972,33**	**322.972,33**
	8	**Serviços especializados de suporte (12 meses)**	horas	300	**288,07**	**980,00**	**634,03**	**190.209,00**
VALOR GLOBAL ESTIMADO DA CONTRATAÇÃO PELA ANEEL (R$) **(1 app. de backup + 8 exp. app. de backup + 8 exp. soft. backup + 8 exp. cybersense* + 8 exp. nsx + serviço de instalação + 300 horas de serviços especializados por 12 meses)**								**5.765.453,40**
OBS: *A ANEEL adquirirá o quantitativo registrado do "item 2 - Módulo de Expansão de Capacidade do DELL Data Domain com garantia e suporte por 60 meses" conforme as suas necessidades durante o prazo de vigência da ATA.*								

3.5.14 Na tabela 5 acima, o valor global estimado da contratação de todos os itens pela ANEEL foi de R$ 5.765.453,40 (cinco milhões setecentos e sessenta e cinco mil e quatrocentos e cinquenta e três reais e quarenta centavos), sendo este valor o resultado do somatório dos valores de cada um dos item da contratação obtidos por meio do cálculo da média aritmética entre os valores unitários médios das contratações obtidas no painel de preços (X) e dos menores valores unitários dos itens obtidos nas propostas comerciais dos fornecedores (Y).

3.5.15 Ressalta-se que a ANEEL poderá contratar o "item 2 - Módulo expansão de capacidade DELL Data Domain" durante o prazo de vigência da Ata e conforme a necessidade de expansão de armazenamento verificada durante a execução do objeto. O item 8 – Serviços de suporte técnico especializados, serão contratados por 12 (meses) e poderão ser prorrogados por iguais e sucessivos períodos, até o limite de 5 (cinco) anos.

4. NORMATIVOS QUE DISCIPLINAM O OBJETO A SER CONTRATADO

4.1 Lei n°8.666/1993, de 21 de julho de 1993, que regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

4.2 Instrução Normativa nº 5, de 27 de junho de 2014, da Secretaria de Logística e Tecnologia e Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MP que regulamenta os procedimentos administrativos básicos para realização de pesquisa de preços;

4.3 Instrução Normativa nº 1/2019, de 4 de abril de 2019, da Secretaria de Governo Digital do Ministério da Economia, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

5. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

5.1 A ANEEL possui vigente o contrato nº 046/2020 cujo objeto é a solução de armazenamento baseado em infraestrutura hiperconvergente, composta por implementação e suporte pelo prazo de 60 (sessenta) meses.

5.2 Dessa contratação supracitada, serão utilizados 4 (quatro) servidores físicos de hiperconvergência fornecidos para a montagem do ambiente de contingência (réplica).

5.3 A ANEEL possui vigente o contrato nº 79/2017 (SICNET 48500.005102/2017-63) cujo objeto é a aquisição de solução de proteção de dados, contemplando o fornecimento de appliance de backup em disco (tipo 1) e módulos de expansão, incluindo os serviços de instalação e configuração, garantia do fabricante e serviços de atualização e suporte técnico pelo prazo de 57 (cinquenta e sete) meses. Esta contratação foi realizada para renovação do ambiente de backup primário da ANEEL, substituindo a antiga solução que fazia uso de armazenamento de dados de backup em fitas magnéticas por um appliance de backup em disco dedicado para este fim.

5.4 Quando da realização dessa contratação, uma vez que não havia um panorama alarmante de ameaças cibernéticas desse tipo para o Brasil, não foi prevista a necessidade de se construir um ambiente de contingência (réplica de backup) para fins de detecção e recuperação de ataques cibernéticos destrutivos.

6. ANÁLISE DA CONTRATAÇÃO ANTERIOR, OU SÉRIE HISTÓRICA

6.1 Não há contratação anterior para a solução de TI em questão.

7. CLASSIFICAÇÃO DO ESTUDO TÉCNICO PRELIMINAR NOS TERMOS DA LEI Nº 12.527/2011

7.1 Não há informações sigilosas caracterizadas nos termos da Lei nº 12527/11 que necessitem a classificação deste documento como reservado, secreto, ultrasecreto.

8. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

8.1 Descrição de solução de TI e declaração de viabilidade da contratação

8.1.1 **Tendo em vista a análise realizada nos itens anteriores deste estudo técnico conclui-se pela viabilidade da contratação da solução descrita a seguir:**

8.1.1.1 Contratação de empresa para fornecimento de ambiente de contingência (réplica de backup de dados) composta por equipamentos (hardwares) e softwares com garantia de 60 (sessenta) meses, incluindo os serviços de implementação (instalação e configuração) e suporte técnico especializados, este último por 12 (doze) meses, renováveis anualmente, por um período de até 60 (sessenta) meses.

8.1.1.2 Sugere-se que esta contratação seja realizada na forma de registro de preços para que a ANEEL possa melhor aproveitar o quantitativo previsto no item 2 do objeto desta contratação à medida que foram sendo necessários durante a vigência da Ata.

8.2 Justificativa para o não parcelamento do objeto

8.2.1 Por se tratar de uma solução que envolve tratamento técnico complexo e que deverá funcionar de forma totalmente compatível e integrada, o parcelamento do objeto não é recomendável uma vez que a eventual divisão dos objetos em lotes diferentes possibilitará que empresas distintas forneçam os componentes da solução.

8.2.2 Dessa forma, o agrupamento dos itens em um único lote mitigará os riscos de integração e compatibilidade da solução. Assim, não haverá como a CONTRATADA alegar no futuro, em caso de

problemas nos equipamentos adquiridos, que os produtos entregues não permitem a interoperabilidade entre si, por serem de outros fabricantes, marcas ou modelos, ficando a ANEEL impossibilitada de penalizar qualquer um destes.

8.2.3 Além disso, não menos impactantes, também poderão ser evitados os seguintes problemas que poderão ocorrer durante a execução contratual desse tipo de objeto com a participação de vários fornecedores:

I. Equipamentos ou serviços parados por aguardar a execução de outro fornecedor;
II. Serviços mal executados em detrimento do outro;
III. Descumprimento dos prazos acordados;
IV. Dificuldade em apontar falhas ou responsabilidades, afetando a entrega do serviço provido pela solução como um todo.

8.2.4 Somando-se a isso, a centralização de responsabilidades promovida pelo agrupamento dos itens em um único lote levará a redução de custos administrativos existentes no gerenciamento de vários contratos e a utilização de diversos mecanismos de controle pela ANEEL, tais como gestores e fiscais.

8.2.5 .Ressalta-se que a contratação de um único licitante por grupo não inviabilizará o atendimento do critério de ampla concorrência do processo licitatório pois existem atualmente no mercado várias empresas especializadas no fornecimento da solução a ser contratada.

8.3 Quantitativos e valores de referência para a contratação:

Valores estimados para a Contratação – Réplica de Backup						
Lote	**Item**	**Descrição**	**Unidade**	**Quantidade**	**Valor Unitário (R$)**	**Valor Total (R$)**
1	1	Appliance de backup "*DELL Data Domain*" com garantia e suporte técnico por 60 (sessenta) meses (equipamento)	unidade	1	**1.419.019,79**	1.419.019,79
	2	Módulo expansão de capacidade do equipamento "*DELL Data Domain*" com garantia e suporte técnico por 60 (sessenta) meses	unidade	2	**550.967,64**	1.101.935,28

		(equipamento)				
	3	Expansão do software de backup "*DELL Data Protection Suite*" com garantia e suporte técnico por 60 (sessenta) meses (licença por processador)	unidade	8	**21.235,00**	169.880,00
	4	Expansão módulo "*Cybersense Data Protection Suite*" com garantia e suporte técnico por 60 (sessenta) meses. (licença por processador)	unidade	120	**1.545.600,00**	1.545.600,00
	5	Expansão do software "*VMWare NSX*" com garantia e suporte técnico por 60 (sessenta) meses (licença por processador)	unidade	8	**72.473,40**	579.787,20
	6	Switch de comunicação de rede LAN com garantia e suporte técnico por 60 (sessenta) meses. (licença por processador)	unidade	2	**218.024,90**	436.049,80
	7	Serviços de implementação da solução	Serviço	1	**322.972,33**	322.972,33
	8	Serviços especializados de suporte	horas	300	**634,03**	190.209,00
VALOR GLOBAL ESTIMADO DA CONTRATAÇÃO PELA ANEEL * (R$)						**5.765.453,40**

** **OBS**: A ANEEL poderá adquirir o quantitativo registrado do "item 2 - Módulo de Expansão de Capacidade do DELL Data Domain com garantia e suporte por 60 meses" conforme as suas necessidades durante o prazo de vigência da ATA.*

8.4 Resultados esperados

I. Garantir a salvaguarda das cópias de segurança das informações eletrônicas críticas contra infecções e perdas definitivas causadas por ataques cibernéticos destrutivos (ransomwares);

II. Garantir a resiliência cibernética dos serviços críticos de TI em caso de desastres causados por ataques virtuais destrutivos (ransomwares);

III. Garantir o fornecimento de infraestrutura com recursos tecnológicos de segurança para as operações críticas de TI adequados ao panorama atual de ameaças cibernéticas;

IV. Operacionalizar as disposições que tratam da continuidade e recuperação de desastres estabelecidas na Política de Segurança da Informação da ANEEL (Norma de Organização ANEEL nº 012) e contidas na NC

06/IN01/DSIC/GSIPR, que estabelece as diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

RESPONSÁVEIS		
IGO RODRIGUES DE CASTRO Analista Administrativo SIAPE: 1912777 Integrante Técnico - SGI	ISSAO HIRATA Superintendente de Gestão Técnica da Informação SIAPE: 3352541 Integrante Requisitante -SGI	ARNALDO JOSÉ FERNANDES JÚNIOR Analista Administrativo SIAPE: 1522568 Integrante Administrativo - SLC
ISSAO HIRATA Superintendente de Gestão Técnica da Informação – SGI Secretário-Executivo da Comissão de Gestão da Informação da ANEEL – CGI		