VALEC ENGENHARIA, CONSTRUÇÕES E FERROVIAS S.A.
DIRETORIA DE ADMINISTRAÇÃO E FINANÇAS
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA/PROJETO BÁSICO

PROCESSO Nº 51402.100731/2020-14

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
01/02/2021	1.0	Finalização da primeira versão do documento	Cláudio Amorim de Sousa
10/02/2021	2.0	Revisão da primeira versão do documento	Luciane Inácia Lopes
27/02/2021	2.1	Revisão prévia de envio ao setor de licitações	Jorge Luis da Silva Lustosa
12/03/2021	3.0	Revisão após análise jurídica	Luciane Inácia Lopes

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de subscrição de licenças de softwares Microsoft, com direito de uso, atualização e suporte, pelo período de 36 (trinta e seis) meses pela VALEC ENGENHARIA, CONSTRUÇÕES E FERROVIAS S.A conforme especificações e quantidades indicadas no quadro a seguir, conforme análise de cenário identificado, documento SEI (51402.100731/2020-14).

1.2. Conforme análise de cenários expressa no documento SEI 3784774, o cenário que atende a demanda da contratação exposta no Documento de Oficialização de Demanda 3781122, apresentando todos os requisitos técnicos expostos nos Estudos Técnicos Preliminares SEI 2743424, 3693150, 3729013, 3715636 e 3715695 e mais vantajoso economicamente segue conforme tabela 01 abaixo:

item	CATSER	SKU	Qtde	Descrição
1	27502	9GS-00495	60	CISSteDCCore ALNG LicSAPk MVL 2Lic CoreLic
2	27502	7JQ-00341	12	SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic
3	27502	AAD-33204	565	M365 E3 Unified ShrdSvr ALNG SubsVL MVL PerUsr
4	27502	1NZ-00004	48	Defender for Endpoint Server SubVL
5	27502	QLS-00003	565	Defender for Endpoint SubVL Per User
6	27502	CE6-00004	565	EntMobandSecE5Full ShrdSvr ALNG SU MVL EntMobandSecE3Full PerUsr
7	27502	NK4-00002	92	Power-BI PRO

Tabela 01 - Licenças Microsoft (SKU)

2. DESCRIÇÃO DAS SOLUÇÕES DE TIC

2.1. As licenças referentes a tabela 01 são compostas por diversos produtos: Microsoft 365 E3, Windows Server Datacenter e System Center, Sistema Gerenciador de Banco de Dados (SGBD), Antivírus Next-Generation, proteção de dados na nuvem (CASB) incluindo mecanismo de Auditoria e PowerBI Pro.

2.2. A solução de licenciamento Microsoft será composta por diversos produtos a serem operacionalizados, sustentados e gerenciados pela VALEC, desde ferramentas de escritório, ferramentas colaborativas, a softwares de sustentação de infraestrutura, através de sistemas operacionais Windows Server Datacenter e de sistema gerenciador de banco de dados (SGBD) - SQL Server, todos estes recursos somando-se a atualização tecnológica através de aplicabilidade de softwares de segurança para Endpoints do tipo Next-Generation Antivirus baseado em comportamento com gerência EDR na nuvem (SaaS), e aplicação de camada de segurança na nuvem para proteção dos ativos da informação da VALEC através de software composto pela solução CASB, incluindo mecanismos de auditoria, em conformidade com a LGPD.

2.3. Demais especificações dos produtos a serem licenciados, encontram-se descritas no **ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO**, deste Termo de Referência.

2.4. As licenças da tabela 01 deverão ser disponibilizadas através de subscrição, com a opção de licenciamento por volume EAS* (Enterprise Subscription Agreement), beneficiando-se do programa SA** "Microsoft Software Assurance".

> *Enterprise Agreement Subscription - Esta modalidade de licenciamento possibilita a utilização de todos os benefícios do Enterprise Agreement. A organização paga por demanda, utilizando os softwares como um aluguel. Este serviço fornece licenciamento por meio de contrato baseado em uma assinatura. Neste contrato, é feito o pagamento do "aluguel" anualmente de acordo com a utilização das licenças. Todos os benefícios de software Assurance serão válidos durante a o período do contrato.
>
> **O SA "Software Assurance" para o Licenciamento por volume inclui uma variedade de benefícios que amplia o software e serviços da Microsoft. O Software Assurance ajuda a impulsionar a produtividade organizacional com suporte técnico 24 horas por dia, 7 dias por semana, serviços de planejamento de implantação, treinamento técnico e para usuários finais, tecnologias e direitos exclusivos e os lançamentos mais recentes de software e de tecnologias exclusivas da Microsoft.

2.5. A opção de licenciamento do tipo EAS traz grandes benefícios para a VALEC, pois também inclui o programa de atualizações das versões de software durante todo o período de vigência contratual, assim como possibilidade de atualização de softwares em servidores, nas estações e utilização da mesma licença para aplicativos na nuvem e em até 5 (cinco) PCs, 5 (cinco) tablets e 5 (cinco) smartfones.

2.6. A “atualização de versão” deve ser entendida como o fornecimento de novas versões corretivas ou evolutivas do software, mesmo em caso de mudança de designação do nome do software, devendo compreender a correção de falhas e implementação de melhorias no produto, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à CONTRATADA.

2.7. As versões das licenças deverão ser as mais recentes disponibilizadas no mercado pelo fabricante.

2.8. As licenças entregues deverão possuir direitos de “downgrade” de forma que uma versão anterior do produto possa ser instalada, a critério da CONTRATANTE.

3. BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

3.1. Toda a solução de licenciamento Microsoft ao serem adquiridas auxiliarão no desenvolvimento das atividades do corpo técnico da VALEC, impulsionando a regra de negócios da Estatal, através da segurança, dinamismo, e versatilidade de softwares baseados em licenciamento de

uso, abrangendo a infraestrutura da VALEC de forma local (on-premises) e através de software como serviço na nuvem. (SaaS) .

3.2. Os produtos que compõem a solução de licenciamento Microsoft são:

a) Suite de escritório Microsoft 365; SEI (2743424);

b) Sistema Gerenciador de Banco de Dados (SGBD) - SQL Server Enterprise 2019; SEI (3693150);

c) Sustentação de Infra para SO's Windows Server Datacenter e Standard 2019;

d) Solução de segurança para Endpoint Next-Generation Antivirus + EDR na nuvem; SEI (3715636);

e) Solução de segurança de Proteção DLP na nuvem + Auditoria (CASB - Cloud Access Security Broker); SEI (3715695)

f) E PowerBi Pro, conforme Item 4.3 deste Termo.

4. JUSTIFICATIVA PARA A CONTRATAÇÃO

4.1. Contextualização e Justificativa da Contratação

4.1.1. A Valec Engenharia Construções e Ferrovias S.A. faz uso intensivo de recursos de tecnologia e segurança da informação e possui um parque de equipamentos diversificado, composto por estações de trabalho, notebooks, dispositivos móveis, armazenamento híbrido, sustentação de infra de servidores, fábrica de software, recursos dispostos na nuvem, dentre outros.

4.1.2. A integração deste conjunto de dispositivos e softwares proporcionam aos usuários da VALEC, desenvolvedores e administradores a execução das atividades laborais de forma dinâmica e segura com acesso aos ativos da informação da VALEC, diretamente na nuvem, com a devida disponibilidade de operacionalização e proteção, incluindo mecanismos de auditoria.

4.1.3. Com o fim da vigência do contrato de fornecimento de licenças Microsoft, faz-se necessária a manutenção das licenças Microsoft ou sua substituição por ferramentas equivalentes que atendam aos requisitos e necessidades da VALEC, considerando a necessidade de manter tal serviço de forma protegida e mais segura, atendendo a novos conceitos de computação em nuvem, atendendo aos normativos de segurança de dados e informações, em acordo com o PSI - Política de Segurança da Informação, e em consonância com a LGPD.

4.1.4. O modelo corrente de contratações pontuais e de soluções próprias, baseadas em investimento em equipamentos e software, está em processo de transformação no serviço público, considerando restrições orçamentárias e a oferta pelo mercado de Software como Serviços (SaaS), Infraestrutura como serviço (IaaS) e Plataformas como Serviço (PaaS).

4.1.5. O modelo de negócios em nuvem, IaaS, SaaS ou PaaS são novos conceitos para a VALEC, que em sintonia, busca a atualização tecnológica, onde alguns serviços já encontram-se dispostos e em operação na nuvem, sendo este modelo de negócio contemplado no PDTI 2019/2021 e recomendado pelo SISP através da IN 01 de 2019 SGD/ME, item 4.1, que trata de instruções para renovação de infraestrutura de centro de dados.

4.1.6. A implantação de software atualizado licenciado e proprietário para acessos aos ativos da informação da VALEC tanto na infraestrutura local (on-premises), quanto através de software como serviço (SaaS) se faz necessária, tendo como intuito facilitar, por exemplo a execução de atividades laborais aos usuários da VALEC, através de suite de escritório inteligente, como Office 365, que funcionam como serviço na nuvem, tendo a possibilidade de trabalhar com o mesmo arquivo na estação ou dispositivo móvel, ambos com sincronismo ativo na nuvem, sendo uma metodologia consonante com a recente modalidade de trabalho, do CAPÍTULO II-A - "DO TELETRABALHO", LEI N. 13.467 da Reforma Trabalhista e em acordo com o item 1 do Anexo da IN 01 de 2019 da Secretaria de Governo Digital, "Contratação de Licenciamento de Softwares e Serviços Agregados".

4.1.7. As demandas por maior produtividade, por processos de trabalho mais integrados e a expansão da modalidade de teletrabalho, exigem que a VALEC forneça soluções que atendam a novos padrões de conectividade e disponibilidade de dados, considerando primordialmente a segurança, tratamento, e privacidade.

4.2. Da ferramenta de "escritório" Microsoft 365 E3:

4.2.1. Atualmente os empregados da VALEC utilizam a solução Microsoft através da suite de escritório Office 365: Word, Excel, PowerPoint, Publisher, Access, Planner, com serviços de e-mail Outlook e ferramentas de colaboração: OneDrive, SharePoint e Teams como serviço na nuvem (SaaS) e com software instalado em desktops e dispositivos móveis.

4.2.2. A necessidade é que toda esta solução seja atualizada a fim de preencher aos requisitos necessários à Valec, considerando a modalidade de contratação de software como serviço (SaaS), garantindo:

I - Versões instaladas e sempre atualizadas;

II - Coautoria em tempo real para que vários usuários possam trabalhar simultaneamente no mesmo documento;

III - Cada usuário pode instalar os aplicativos de suite de escritório em mais de um dispositivo;

IV - Versões Web dos aplicativos Word, Excel e PowerPoint, Outlook e de toda suíte office;

V - Versões sempre atualizadas dos aplicativos Word, Excel, PowerPoint ou equivalentes para dispositivos iOS e Android;

VI - Hospedagem de e-mail com caixa de correio de 100 GB.

4.2.3. A suite Office Microsoft 365 consiste em uma solução de produtividade e colaboração da Microsoft, disponibilizada em ambiente de nuvem, que integra aplicativos e recursos digitais com vistas a proporcionar ferramentas que possibilitem o aumento da eficiência na realização de atividades comuns relacionadas à produção digital de conteúdo e na organização e comunicação dentro das equipes de trabalho.

4.2.4. O plano Office 365 E3 destina-se a funcionários com perfil de uso do suite E1 mais direito de uso dos aplicativos na versão web e no dispositivo Word, Excel, PowerPoint, OneNote, Outlook, Exchange, OneDrive for Business, Teams, Access (PC apenas), Publisher (PC apenas), SharedPoint, Yammer, Stream, Sway, Delve, Microsoft Froms, Planner, To Do, Power Virtual Agents paraTeams incluindo licença para uso dos aplicativos em até 15 dispositivos por usuário: 5 (cinco) para estações Windows ou Mac 5 (cinco) para smartphones e 5 (cinco) para tablets, espaço na nuvem de 5 TB por usuário, Microsoft Intune, funções de proteção de dados, como: criptografia de mensagens, direitos de gerenciamento, e DLP para e-mail e arquivos.

4.2.5. O Core CAL Bridge for Office 365 é um tipo de licença de subscrição que garante o direito de acesso aos serviços do Office 365 para um determinado *client* (usuário ou dispositivo).

4.2.6. O plano Microsoft 365 F3 destina-se a funcionários com perfil de uso dos aplicativos apenas versão web do Word, Excel, PowerPoint, OneNote, Outlook, OneDrive for Business, Teams, SharePoint, Yammer, espaço na nuvem de 2 GB por usuário, Microsoft Intune, funções de proteção de dados, como: criptografia de mensagens básica, Windows Defender Antivirus - Device Guard, direitos de gerenciamento na nuvem.

4.2.7. O plano Microsoft 365 E3 destina-se a funcionários com perfil de uso do suite F3 mais direito de uso dos aplicativos na versão web e no dispositivo Word, Excel, PowerPoint, OneNote, Outlook, OneDrive for Business, Teams, Access, SharedPoint, Yammer, Stream, Sway, Lists, incluindo opções de instalação dos aplicativos em até 5 dispositivos por usuário: Windows, Mac, Android, tablets e smartphones, espaço na nuvem de 5 TB por usuário, Microsoft Intune, funções de proteção de dados, como: criptografia de mensagens, direitos de gerenciamento, e DLP para e-mail e arquivos.

4.2.8. O plano Microsoft 365 E5 destina-se a funcionários com perfil de uso do suite E3 mais direito de uso dos aplicativos na versão web e no dispositivo Word, Excel, PowerPoint, OneNote, Outlook, OneDrive for Business, Teams com recurso de chamada pública, Access, SharedPoint, Yammer, Stream, Sway, Lists, Power BI Pro, incluindo opções de instalação dos aplicativos em até 15 dispositivos por usuário: 5 (cinco) para estações Windows ou Mac 5 (cinco) para smartphones e 5 (cinco) para tablets, Microsoft Intune, funções de proteção de dados, como: criptografia de mensagens, direitos de gerenciamento, e DLP para e-mail e arquivos, proteção ativa contra ameaças anti-malware Next-Generation ATP, proteção Cloud App Security (solução CASB).

4.2.9. A suite Microsoft 365 E3 em comparação a suite Office 365 E3, tem como principal diferencial o pacote **Azure Active Directory Premium P1**, desenvolvido para elevar a gerência de identidade na nuvem, propiciando ao usuário recursos self-service para identidade e gerência de acesso (IAM), reset de senha on-line, multi-fator de autenticação, atualização de informações da conta, além de recursos de Ingresso no Azure AD (Join) na nuvem, sincronismo com o AD on-premises (Azure AD Connect sync), registro de dispositivo, gerenciamento de grupos para condicionar acessos através de termo de uso, multi-fator de autenticação, SharePoint limitação de acesso, condição baseada em grupo, localização e status do dispositivo, descobrimento de aplicações através do Microsoft Cloud App Discovery, aplicabilidade de segurança através de integração de autenticação Single Sing-On (SSO), autenticação por federação (ADFS or IdP) para integração de soluções de terceiros.

4.2.10. Ainda, com o uso do SKU CE6-00004 (EntMobandSecE5Full ShrdSvr ALNG SU MVL EntMobandSecE3Full PerUsr), têm-se a vantagem quanto a proteção de identidade do usuário na nuvem adicionando o pacote **Azure Active Directory Premium P2**com os seguintes recursos: "detecção de risco de vulnerabilidade de contas", "investigação de eventos de risco" , "políticas de acesso condicional baseado em risco", ainda para gestão de governança de identidade têm-se os recursos: "Gerência de identidade e privilégios (PIM), "Revisão de Acesso" e "Gerência de Direitos".

4.2.11. Faz-se necessário a escolha do uso do licenciamento da Microsoft, devido ao fato da VALEC ter feito investimento na suite de ferramentas de escritório da Microsoft, ao qual, os usuários tiveram treinamento, assim como o fato da suite Microsoft 365 ser uma ferramenta robusta e adequada às necessidades da empresa, tanto para o ambiente em nuvem quanto para o ambiente local (on-premises).

4.2.12. Em torno desses softwares, foi construído todo o conjunto de ferramentas e sistemas responsáveis tanto para utilização na infraestrutura local quanto em nuvem contribuindo para automação dos fluxos de trabalho da VALEC e das Unidades Descentralizadas.

4.3. **Das licenças do Power-BI Pro**

4.3.1. O Power BI facilita a visualização e o entendimento das informações do negócio e com isso facilitar também as tomadas de decisão. Com elementos visuais como gráficos e indicadores de gestão permitem que tanto os gestores, quanto equipe consigam monitorar o andamento de metas e resultados com mais clareza, pois são elementos altamente interativos, dinâmicos, customizáveis e intuitivos. Sua utilização na Valec tem sido cada vez mais efetiva, ficando porém limitada à sua versão gratuita. Torna-se necessário a subscrição dessa ferramenta que tem sido demanda por gestores e analistas de áreas críticas para a Valec.

4.3.2. A utilização dessa ferramenta visa auxiliar e a implementar uma governança e acompanhamento mais efetivo de todas as ações e resultados de uma forma gráfica e de fácil entendimento, permitindo o aumento da produtividade e tomadas de decisões assertivas.

4.3.3. Esta solução Microsoft foi incorporada a presente contratação tendo em vista o atendimento da demanda oficializada pelo DOD aproveitando-se da vantajosidade econômica na subscrição de um conjunto de licenças Microsoft, objeto desta contratação.

4.3.4. Segue resumo, quadro abaixo, do uso das 92 licenças para o Power-BI Pro:

Perfil (usuário)	Quantidade
Gerentes	47
2 licenças adicionais por superintendência a serem distribuídas sob demanda aos empregados do setor	30
Superintendentes e Assessores	15
Total	**92**

4.3.5. Das versões Power-BI:

4.3.5.1. O Power BI Desktop é um aplicativo gratuito que é instalado no computador local onde é possível combinar diversas fontes de dados. Com ele é possível fazer diversos tipos de gráficos, tabelas e filtros, inserir imagens, trabalhar com figuras e transformar seus dados em informação visual. Possibilitando criar relatórios e dashboards que facilitam a análise e a tomada de decisão. Todo trabalho feito no Power BI Desktop é salvo no computador local, e pode ser visualizado online através do Power BI Service.

4.3.5.2. O Power BI Service é o serviço online do Power BI. Através dele é possível compartilhar relatórios e dashboards com outros membros da organização. Os relatórios podem ser apenas visualizados, ou editados por outros usuários autorizados, o que acelera o fluxo de informação dentro da empresa.

4.3.5.3. Na sua interface é possível trabalhar com os relatórios vindos do Power BI Desktop ou criar relatórios novos, através da importação e trabalho das bases de dados diretamente nesta ferramenta.

4.3.5.4. O Power BI Mobile está disponível para dispositivos móveis com iOS, Android e Windows. Através dessa plataforma é possível conectar e interagir com os dados locais e da nuvem, ou seja, é possível acessar os relatórios criados no Power BI Desktop e no Power BI Service. Essa é a forma de ter o Power BI ao acesso da mão, no seu celular, ter as informações em tempo real é um grande diferencial na gestão dos negócios.

4.3.5.5. Com o Power BI Pro é possível publicar os relatórios no Power BI Service, ou seja, com essa licença é possível conectar-se diretamente aos dados locais ou em nuvem, em tempo real. Além disso é possivel compartilhar relatórios com usuários de dentro e fora da organização.

4.4. **Das características de segurança para proteção de Antivírus Next-Gen, e proteção DLP na nuvem e auditoria (CASB)**

4.4.1. Sabe-se que a exploração de vulnerabilidades e tentativas de furto de informações em cibersegurança é uma realidade iminente.

4.4.2. Faz-se necessário a aquisição de software de segurança a fim de atender a proposta das duas infraestruturas, on-premises e na nuvem (IaaS), através da aquisição de softwares por meio de cessão temporária de direito de uso (subscrição) para endpoints em infraestrutura *on-premises* (local) usando a tecnologia Next-Generation Antivirus, e proteção dos ativos da informação e aplicações na nuvem através da solução CASB contra ameaças provenientes de dispositivos corporativos (gerenciados) e pessoais (não-gerenciados), somando-se aos recursos de auditoria dos acessos na infra da nuvem (IaaS).

4.4.3. A implantação por um modelo híbrido de proteção para endpoint e ativos da informação na nuvem são necessários, devendo-se considerar o novo modelo de negócios da VALEC tanto na infraestrutura local (on-premises), quanto na infraestrutura em nuvem (IaaS).

4.4.4. A PSI - Política de Segurança da Informação da VALEC, estabelece através do item 2.3, do Objeto *"Prevenir possíveis causas de incidentes, com possível responsabilização da instituição e de seus empregados, clientes e parceiros, e ainda, minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da VALEC advindo como resultado de falhas de segurança."*, desta forma, faz-

se necessário proteger os ativos da informação da VALEC através de software de segurança para endpoints, estabelecendo uma camada de proteção ativa para estes, respectivamente através de mecanismo de proteção baseado em comportamento usando inteligência artificial (machine learning).

4.4.5. Com intuito de proteger a atividade de negócios da VALEC, faz-se necessária a atualização tecnológica do software endpoint contra *malwares* baseado em comportamento e não mais em assinatura, do tipo Next-Generation Antimalware que possui engenharia mais eficiente, sendo o agente mais leve (agent lightweight), não havendo a necessidade de varredura, oferecendo mecanismo de detecção, desempenho, e gerenciamento centralizado, tendo proteção baseada em inteligência artifical - *machine learning* para proteções de malwares do tipo: Ransonware, Trojan, Spyware, Adware, Worms, rootkits, keyloggers, dentre outros.

4.4.6. A solução de segurança para endpoint Next-Generation deve proteger todos os dispositivos corporativos da VALEC, ou seja, computadores, notebooks, e servidores no acesso a infraestrutura on-premises (local) e serviços que compõem a infraestrutura.

4.4.7. Já a solução CASB (Cloud Access Security Broker), esta possui a premissa de que todos os dispositivos que se conectem aos serviços da VALEC na nuvem, não são confiáveis (zero trust), e não possuem agente instalado (agentless) onde a solução faz a checagem dos dispositivos na pré-autenticação da sessão, atuando como broker (proxy), através de políticas a serem definidas para proteção das aplicações e dados sensíveis na nuvem fazendo a proteção contra vazamento de dados DLP (Data Loss Prevention), atuando na proteção de encriptação de arquivos, assim como na restrição do uso de aplicações não homologadas pela VALEC que possam inferir na camada da nuvem, contaminando-a, por exemplo, através de upload do arquivo contaminado, dentre outras funcionalidades descritas nas sessão de especificações, a seguir.

4.4.8. A infraestrutura em nuvem (IaaS) é um novo conceito para a VALEC, onde alguns serviços encontram-se dispostos e em operação na nuvem, a exemplo, a suite Office 365 (SaaS) disposta pelo provedor Microsoft, composta por ferramentas de escritório: Word, Excel, PowerPoint, Project e softwares de colaboração: MS Teams, MS OneDrive, MS Shared Point, tendo os arquivos armazenados nesta estrutura.

4.4.9. Assim como a proteção dos ativos da informação da VALEC, a Auditoria para o acesso a informação através dos dados dispostos na infraestrutura em nuvem (IaaS) faz-se necessária utilizando a mesma solução, CASB, visto que, parte da estrutura de ativos da informação fora transferida para a nuvem como citado no item 4.4.8, sendo criterioso a auditoria na gestão de identidade, assim como na gestão de controle de acesso contra vazamento de dados (DLP) através de políticas configuráveis na solução.

4.4.10. Na proposta de aquisição das licenças Microsoft, tabela 01 item 6, este licenciamento traz módulos vitais a suite de escritório Microsoft 365 E3 que propiciam funcionalidades de segurança e mobilidade corporativa em integração à solução (EMS - Enterprise Mobility Security), como:

I - Microsoft Intune;

II - Gerenciamento de dispositivos móveis;

III - Microsoft Defender of Identity;

IV - Multi-factor de autenticação;

V - Windows AutoPilot;

VI - Azure Active Directory Premium Plan 2;

VII - Microsoft Cloud APP Security (CASB);

VIII - Criptografia de mensagens básica do Office;

IX - Política de retenção do Teams

X - Análise de ameaças avançadas da Microsoft;

XI - Dentre outras.

4.4.11. O licenciamento das soluções Microsoft, engloba a proteção para endpoints e proteção contra vazamento de dados na nuvem contendo mecanismos de auditoria com necessidade de integração através dos seguintes softwares: (1) MS Defender ATP e (2) MCAS (MS Cloud APP Security), sendo extremamente necessárias para segurança cibernética da VALEC, propiciando:

I - Proteção dos ativos da informação da VALEC através de solução de segurança CASB (SaaS) para proteção dos ativos da informação na nuvem (IaaS) contra ameaças provenientes de dispositivos gerenciado e não-gerenciados (agentless);

II - Criar camada de proteção contra malwares na infraestrutura de nuvem para proteger os ativos da informação da VALEC a fim de garantir a integridade, disponiblidade e confidencialidade;

III - Ampliar o nível geral de segurança dos ativos da informação da VALEC, em conformidade com as mudanças realizadas na infraestrutura da rede local e na nuvem da VALEC;

IV - Aplicar mecanismos de proteção contra vazamentos de dados (DLP) na nuvem (IaaS);

V - Aplicar mecanismos de auditoria através de ferramenta integrada a solução CASB no acesso as informações dispostas na nuvem em acordo com a LGPD.

4.4.12. Cabe salientar a importância da integração das soluções Microsoft Defender ATP (Advanced Threat Protection) e MS Cloud App Security (MCAS), dentre elas, destacam-se:

I - A solução Microsoft Defender ATP (Advanced Threat Protection), integra-se a solução MS Cloud App Security (MCAS) sendo possível bloquear o acesso a URL's ou endereços através do Microsoft Cloud App Security (MCAS);

II - Bloqueio a determinadas URL's diretamente no dispositivo mesmo fora da organização, não sendo necessário aplicar o bloqueio em ativos como firewalls, proxies, e em nível de DNS;

III - Aplicação de regras condicionais para o Cloud App Security, baseadas na verificação do Agent do MS Defender ATP no endppoint;

IV - A verificação de propensos arquivos infectados ao qual o usuário faria o (upload) passando pelo MCAS, não necessita de verificação pelo MCAS, poupando recursos, devido ao endpoint já possuir o agente Antivirus MS Defender ATP; (zero-trust)

V - O Cloud App Security usa as informações de tráfego coletadas pelo MS Defender ATP sobre os aplicativos e serviços em nuvem acessados a partir de dispositivos Windows 10 gerenciados pela TI. A integração nativa permite que você execute o Cloud Discovery em qualquer dispositivo da rede corporativa, usando Wi-Fi público, em roaming e por acesso remoto. Ele também permite a investigação baseada no dispositivo;

VI - O Cloud App Security coleta os logs dos endpoints. A integração nativa traz a vantagem quanto a descoberta de Shadow IT em dispositivos Windows em sua rede;

VII - Os aplicativos marcados como não-sancionados no MS Cloud App Security (MCAS) são automaticamente sincronizados no MS Defender Endpoint, geralmente levando alguns minutos. Mais especificamente, os domínios usados por esses aplicativos não-sancionados são propagados para dispositivos de endpoint para serem bloqueados pelo Microsoft Defender Antivirus dentro do SLA de proteção de rede.

VIII - Integração entre o serviço de identifidade do Microsoft Azure AD;

IX - Dentre outras.

4.4.12.1. **Da integração da solução a suite de escritório Office 365, são necessárias as seguintes remediações em eventos de DLP e segurança:**

I - Excluir um arquivo e pasta violado para a lixeira do administrador;

II - Colocar o arquivo e pasta violada na quarentena do administrador;

III - Colocar o usuário em quarentena;

IV - Remover o colaborador específico;

V - Remover permissão específica de um arquivo ou pasta do Office 365, revertendo a permissão na pasta herdada (pai);

VI - Habilitar eventos de auditoria do Exchange no Office 365, quando um usuário for definido com privilégios administrativos possibilitando a visualização de alertas no solução CASB;

VII - Rastrear atividades de usuário no Power-BI;

4.4.12.2. **Ainda, da integração da solução CASB com o Azure Active Directory:**

I - Notificar o usuário através de alerta via Azure AD;

II - Requere que o usuário faça login novamente via Azure AD;

III - Suspender o usuário via Azure AD;

IV - Capacidade de integrar-se ao log de eventos de identidade do Azure AD Identity Protection;

V - Mostra alertas de vazamento de credenciais;

VI - Agregar várias detecções de tentativas de falhas de login que não foram realizados pelo usuário;

VII - Sincronismo de logs de eventos de segurança do Azure AD Identity Protection;

VIII - Integração nativa com a "Proteção de Identidade" do Azure Active Directory (Azure Active Directory Identity Protection) possibilitando identificar análise de comportamento;

4.5. **Do Sistema de Gerenciamento de Banco de Dados (SGBD)**

4.5.1. Há diversos sistemas na VALEC, tanto de terceiros quanto desenvolvidos internamente, que dependem do SQL Server. Os sistemas que usavam o SGBD Oracle estão em fase final de conversão para o SGBD da Microsoft. Após o fim da conversão, demais aplicações que ainda não estavam sob a plataforma SQL Server, como SOS - Sistema de Ordem de Serviços, ForPonto - Ponto Eletrônico, SINUDO - Numeração de documentos, SIOCA - Sistema de Ocorrências Ambientais, SISAUDIN - Auditoria Interna, SICOD - Desapropriações, SIPAV - Permissões e Autenticações, SRB - Reembolso de Benefícios, SISTEL - Lista Telefônica, Controle de Patrimônio, Controle do Almoxarifado, ARCGIS - Sistema de Informações Geográficas, entre outros, necessitarão do SQL Server;

4.5.2. É necessário ter o suporte para este SGBD, que inclui a disponibilização de *patches* corretivos, evolutivos e de segurança da ferramenta, cuja operacionalização é vital para armazenamento dos dados dos sistemas referenciados no item 4.5.1;

4.5.3. Sem o licenciamento/suporte contratado, não se tem a garantia de correção de erros/bugs da ferramenta e nem apoio técnico especializado para solução de problemas que possam surgir, afetando os usuários dos sistemas e, por consequência, a missão da VALEC;

4.5.4. Na tabela 01, conforme item 2, foi especificado o quantitativo de 12 licenças SQL Enterprise (QLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic), que equivalem a concessão de 24 CPU's, justificado pois essa é a quantidade atual de núcleos/cores dos equipamentos servidores que sustentam o ambiente de bancos de dados (SGBD) institucionais da VALEC, número este que atende as demandas de desempenho/capacidade solicitadas pelas equipes demandantes.

4.5.5. Ainda, cabe ressaltar que neste cálculo é considerado o número de instâncias e/ou bases de dados existentes licenciados por número de núcleos/cores do servidor VM para as instâncias de Produção (10), Homologação (4), Report Server (6), e futura utilização de instância de desenvolvimento (4) considerando a contratação da fabrica de software.

4.5.6. A versão SQL Server 2019 traz importantes atualizações tecnológicas em relação à versão SQL Server 2017 usada atualmente pela Valec. Em geral, essas atualizações traduzem-se em incremento da produtividade de funções relativas à gerência do SGBD. Destaca-se aqui algumas características da última versão do SGBD:

4.5.6.1. Melhoramentos no processamento inteligente de queries (Intelligent Query Processing). É um conjunto de melhorias que afetam o comportamento do otimizador de consultas;

4.5.6.2. Recuperação acelerada de banco de dados (Accelerated Database Recovery - ADR). São ferramentas totalmente reescritas para proceder recuperações nos casos de desfazimento de transações, reinício de instâncias ou falha na disponibilidade. Os tempos de processamento das funções envolvidas reduziram-se tremendamente;

4.5.6.3. Encriptação com enclaves seguros (AlwaysEncrypted with secure enclaves). O SQL Server agora pode encriptar porções de memória para trabalhar com colunas encriptadas sem expor os dados a outros processos ou para administradores;

4.5.6.4. Tempdb de Metadados otimizada para uso em memória (Memory-optimized Tempdb metadata). O acesso aos metadados na Tempdb, que poderia tornar-se um gargalo em sistemas com uso pesado desta funcionalidade, pode ser feito completamente em memória;

4.5.6.5. Políticas de captura da Query Store personalizáveis (Query Store custom capture policies). A Query Store é uma ótima ferramenta de ajustes finos no BD que nesta versão ganha opções de uso que a tornam melhor ainda;

4.5.6.6. Avisos de truncamento mais explicativos (Verbose truncation warnings). Os desenvolvedores ganharão tempo procurando a origem de erros de truncamento;

4.5.6.7. Construção retomável de índices (Resumable index build). Na versão mais nova é possível parar e retomar a qualquer tempo a construção de índices;

4.5.6.8. Virtualização de dados com Polybase. Polybase é o modo do SQL Server que permite a consulta a dados externos, em outros SGBDs. Ele foi extendido para suportar Oracle, Teradata, MongoDb e outros.

4.5.7. Ainda, com o advento do sistema DTE (Documento de Transporte Eletrônico), faz-se necessário o correto dimensionamento da quantidade de CPU's licenciada para o SGBD a fim de garantir a performance e aplicação de alta disponibilidade (HA - High Availability) para as transações que ocorrerão em território nacional, em tempo real.

4.6. **Do licenciamento Windows Server Datacenter**

4.6.1. O licenciamento CIS Datacenter consiste na concessão para uso em infraestrutura virtualizada, licenciando hosts físicos por CPU, assim como licencia número ilimitado de máquinas virtuais (VM's) para o sistema operacional Windows Server Standard, e operação do Sistema System Center.

4.6.2. Na estrutura de virtualização de infraestrutura de servidores da VALEC, este tipo de licenciamento permite a flutuação das máquinas virtuais entre os hosts físicos, proporcionando elevada performance no processamento das máquinas virtuais, permitindo a eficiência na utilização de recursos de hardware, através de balanceamento das vms entre os hosts físicos, garantindo a eficiência, a integridade, disponibilidade e confiabilidade de operação para o ambiente de produção no Datacenter da VALEC.

4.6.3. O Sistema System Center é responsável pelo gerenciamento de servidores e de

estações de trabalho, inventário de software e de hardware, aplicação de patches de segurança, deploy de software, elaboração de relatórios e verificação da aderência de cliente a critérios de Compliance. Tal sistema garante o gerenciamento de todo o parque tecnológico dos dispositivos de usuários, computadores e notebooks, que utiliza o Sistema Operacional Windows no ambiente da Valec.

4.6.4. Na tabela 01, no item 1, foi especificado o quantitativo de 60 licenças 2-packs, que resultam em 120 licenças (120 CPU's), ou seja, cobrem a utilização de dois hosts físicos com 60 CPU's cada, permitindo a operação ilimitada de máquinas virtuais (VM's) em ambiente virtualizado.

4.6.5. A VALEC atualmente faz uso de servidores de rede e de máquinas virtuais, utilizando 160 máquinas virtuais, sendo 48 com o sistema operacional Windows Server.

4.6.6. O Sistema Operacional Windows Server é de fundamental importância para a organização, pois suporta parte dos principais serviços e sistemas que apoiam a execução das atividades finalísticas da Valec. São exemplos de serviços internos e sistemas que funcionam sobre Sistemas Operacionais Windows Server:

- Aplicação interna da Telefonia;
- Servidor AD, DNS, DHCP, TimeServer e NPS;
- Nuvem Office 365 (Azure Connect);
- Servidor WEB FORPONTO ;
- SQL Report Services;
- System Center Configuration Manager (SCCM)
- Sharepoint
- Autoridade Certificadora Interna;
- Assyst;
- Varonis;
- SQL Server;
- Aplicativos de RH;
- File Server;
- Servidor de Orçamento de Obras Compor90;
- QUANTM
- E outros correlatos.

4.6.7. Mesmo com a utilização de soluções gratuitas em algumas máquinas virtuais hoje instaladas no ambiente da Valec, algumas aplicações e serviços utilizados internamente, como os informados acima, tem como requisitos a instalação em ambiente Windows, tornando assim necessário seu licenciamento.

4.6.8. De modo geral, a interrupção do suporte e do direito de atualização destas licenças, eleva o risco de indisponibilidade de diversos sistemas e soluções informatizados, que são críticos para área de negócio da VALEC.

4.6.9. O Windows Server permitirá pelo menos dois acessos simultâneos à Área de Trabalho Remota pelos administradores do Sistema Operacional.

4.6.10. Será gerenciável a partir do System Center Configuration Manager (SCCM), que já é utilizado pela VALEC e, dentre outros aspectos, permitirá:

- Gerenciamento de servidores e de estações de trabalho
- Inventário de software e de hardware
- Aplicação de patches de segurança
- Deploy de software
- Elaboração de relatórios
- Verificação da aderência de cliente a critérios de *Compliance*

4.7. **Alinhamento aos Instrumentos de Planejamento Institucionais**

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
OE TIC 01	Aprimorar continuamente a experiência dos serviços prestados aos clientes
OE TIC 02	Expandir a prestação de serviços digitais
OE TIC 06	Fomentar a cooperação e o entendimento mútuo entre a TIC e as áreas de negócios objetivando a agregação de valor
OE-TIC-05	Integrar dados, processos, sistemas, serviços e infraestrutura
OE-TIC-04	Aprimorar os níveis de maturidade em Gestão e Governança de TIC com a adequação às melhores práticas do mercado
OE-TIC-04	Prover Segurança da Informação, garantindo a disponibilidade, confiabilidade e integridade das informações prestadas ao público interno e externo da VALEC

ALINHAMENTO AO PDTIC VIGENTE			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
2	Expandir a prestação de serviços digitais	1	Executar o projeto de expansão dos serviços digitais.

4.8. **Estimativa da demanda**

4.8.1. Conforme justificativas para a demanda, seguem tabela demonstrativa der licenças com a respectiva SKU:

Lote/Grupo	item	CATSER	SKU	Qtde	Descrição
1	1	27502	9GS-00495	60	CISSteDCCore ALNG LicSAPk MVL 2Lic CoreLic
	2	27502	7JQ-00341	12	SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic
	3	27502	AAD-33204	565	M365 E3 Unified ShrdSvr ALNG SubsVL MVL PerUsr
	4	27502	1NZ-00004	48	Defender for Endpoint Server SubVL
	5	27502	QLS-00003	565	Defender for Endpoint SubVL Per User
	6	27502	CE6-00004	565	EntMobandSecE5Full ShrdSvr ALNG SU MVL EntMobandSecE3Full PerUsr
			NK4-		

	7	27502	00002	92	Power-BI PRO

4.9. **Parcelamento da Solução de TIC**

4.9.1. A solução é composta por diversos itens que, por suas características técnicas, na sua grande maioria, poderiam ser divididos em diversas parcelas. Contudo, devido à estrutura comum de integração das soluções ao contrato com formato Enterprise Subscription Agreement, a fabricante da solução concede condições diferenciadas devido à padronização dos softwares do parque computacional que não podem ser segregados em contratos distintos. A alternativa a essa opção é a contratação de licenças do tipo Open ou Select, que não garantem o mesmo nível de desconto dos valores e não disponibiliza diversas aplicações e funcionalidades necessárias ao bom funcionamento dos sistemas e ao pleno atendimento das demandas.

4.9.2. A opção contratação de licenças do tipo Open ou Select, apesar de ampliar o universo de empresas participantes, não implicará em ganho para a administração pública pelo aproveitamento dos recursos disponíveis no mercado, haja vista que a forma de licenciamento disponível para essas empresas, Select e Open, não atingem o mesmo nível de desconto do fabricante e não compõem uma solução adequada para atendimento das necessidades do serviço público.

4.9.3. Com isso, a divisão vai de encontro ao que a Lei nº 13.303, de 2016, que descreve em seu art. 32, Inciso III, por não permitir a administração pública obter valores menores devido a economia de escala e à viabilidade técnica da solução:

> "III - parcelamento do objeto, visando a ampliar a participação de licitantes, sem perda de economia de escala, e desde que não atinja valores inferiores aos limites estabelecidos no art. 29, incisos I e II;"

4.9.4. Como os itens que compõem o grupo 01 desta contratação possuem a mesma natureza e relação entre si, o que torna seu parcelamento técnica e economicamente inviável. A adjudicação do grupo 01 desta contratação a empresas distintas, além de aumentar seu custo administrativo prejudica a economia de escala na contratação.

4.9.5. Desta forma, os itens devem ser contratados de maneira agrupada em lote único para composição de contrato Enterprise Agreement Subscription .

4.10. **Resultados e Benefícios a Serem Alcançados**

4.10.1. Agilidade e disponibilidade de serviços computacionais;

4.10.2. Soluções integradas de comunicação colaborativas, incluindo sessões áudio e vídeo;

4.10.3. Ferramentas integradas que oferecem a disponibilidade de informações em tempo real como serviço na nuvem (SaaS);

4.10.4. Integração de todas as ferramentas com o ambiente de rede de serviço local (on-premises) e na nuvem pelo Azure Active Directory;

4.10.5. Gerenciamento administrativo de dispositivos corporativos, e pessoais (BYOD) em nuvem através do Microsoft Intune;

4.10.6. Sistemas operacionais servidores com serviço de virtualização e cluster para disponibilidade e tolerância a falhas das máquinas virtuais instaladas no ambiente.

4.10.7. Sistema de gerenciamento de ambiente virtual;

4.10.8. Sistema de SGBD robusto e inteligente para comportar instâncias de aplicações incluindo futuro projeto DTE.

4.10.9. Proteção de endpoints Next-Generation Antivírus;

4.10.10. Proteção contra vazamento de dados (DLP) na nuvem e auditoria;

5. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

5.1. **Requisitos de Negócio**

5.1.1. Garantir continuidade e a capacidade de atendimento às áreas de negócio da VALEC, que dependem das soluções de tecnologia da informação.

5.1.2. Fornecer às unidades de negócio da VALEC e à sociedade soluções tecnológicas que agreguem valor ao negócio e atendam às necessidades do cidadão no fornecimento de informações e serviços disponibilizados com qualidade e eficiência;

5.1.3. Atualização do licenciamento Microsoft e aplicação de novas tecnologias no âmbito da VALEC;

5.1.4. Preservação dos investimentos já realizados pela VALEC em seu parque computacional baseado em produtos Microsoft;

5.1.5. Manutenção e evolução das aplicações e soluções desenvolvidas pela VALEC adicionando novas exigências, facilidades e aprimoramentos;

5.1.6. Padronização dos produtos de software modernizando, em tempo hábil, considerando o parque computacional e serviços em nuvem aplicados à VALEC, manutenção da prestação dos serviços e retenção do conhecimento técnico adquirido nessa plataforma;

5.1.7. Utilização de novas funcionalidades dos produtos Microsoft considerando a segurança da informação, projetados para atender às necessidades de, confiabilidade, integridade, disponibilidade e produtividade do usuário tanto na infraestrutura local (on-premises), como através de serviços na nuvem (SaaS) atendendo suas exigências de maior mobilidade, seja através de dispositivos em ambiente corporativo, através de estações de trabalho, notebooks, tablets, quanto remoto, possibilitando a utilização dos serviços em celulares, smartphones e demais equipamentos móveis;

5.1.8. Acesso aos produtos Microsoft e dados dos usuários em vários dispositivos, mesmo fora do ambiente da VALEC, proporcionando maior colaboração e trabalho à distância.

5.2. **Requisitos de Capacitação**

5.2.1. A capacitação em ferramentas Microsoft não faz parte do escopo desta contratação tendo em vista que o objeto desta diz respeito à contratação de serviços e de subscrição de licenças MICROSOFT.

5.3. **Requisitos Legais**

5.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, ao Decreto-Lei nº 200/1967, à Lei nº 13.303, (Lei de Licitações), à Lei nº10.520/01, (Lei do Pregão), ao Decreto nº 10.024/2019 (Pregão Eletrônico), à IN SGD-ME nº 01/2019 (Contratação de Soluções de TIC), Regimento Interno de Licitações e Contratos, RILC/2021 Valec e a outras legislações aplicáveis.

5.4. **Requisitos de Manutenção**

5.4.1. Direito de atualização de software, pacotes de correção, e upgrade do produto para a última versão estável através de benefício SA "Software Assurance".

5.4.2. **Requisitos Temporais**

5.4.3. A reunião inicial de alinhamento deverá ocorrer após a assinatura do contrato e ser executada em, no máximo, 5 (cinco) dias úteis após a assinatura do contrato.

5.4.4. O prazo de vigência e execução do contrato será de 36 (trinta e seis) meses a contar da emissão da Ordem de Serviço.

5.4.5. A CONTRATADA terá o prazo de até 5 (cinco) dias úteis para realizar a disponibilização das licenças a partir da entrega da OS.

5.4.6. Após a ativação, a CONTRATADA deverá apresentar, no prazo de 2 dias úteis, relatório demonstrativo das licenças disponibilizadas.

5.4.7. As novas versões das subscrições de licenças adquiridas, deverão ser disponibilizadas em até 15 (quinze) dias, a partir do lançamento oficial da nova versão.

5.5. **Requisitos Sociais, Ambientais e Culturais**

5.5.1. A CONTRATADA deverá fornecer as licenças de software de forma eletrônica, evitando a confecção e transporte de mídias;

5.5.2. Os profissionais da CONTRATADA, quando presentes nas instalações da CONTRATANTE, deverão apresentar-se vestidos de forma adequada ao ambiente de prestação dos serviços (trabalho), evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da VALEC, ou que ofenda o senso comum de moral e bons costumes;

5.5.3. Os profissionais da CONTRATADA deverão respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;

5.5.4. A prestação de serviços objeto deste Termo de Referência não gera vínculo empregatício entre os empregados da CONTRATADA e a CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação.

5.5.5. 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.

5.5.6. Todos os softwares devem possuir suporte aos seguintes idiomas: Inglês ou Português Brasileiro a ser definido pela contratante.

5.6. **Requisitos de Arquitetura Tecnológica**

5.6.1. A arquitetura tecnológica da solução deverá observar os requisitos específicos de cada item de acordo com as especificação técnica constantes no Anexo I deste Termo de Referência, e:

5.6.2. Ter compatibilidade entre os diversos aplicativos e serviços que compõem a solução, por serem do mesmo fabricante e serem comercializados em conjunto;

5.6.3. Grande cobertura de funcionalidades de automação de escritório e de trabalho em equipes;

5.6.4. Possuir oferta frequente de novas funcionalidades, melhorias e correções de bugs;

5.6.5. Consistência da estrutura de suporte técnico à disposição para a solução;

5.6.6. Ampla disponibilidade de treinamento para usuários e profissionais de TI no que concerne ao uso e suporte da solução.

5.7. **Requisitos de Projeto e de Implementação**

5.7.1. Não se aplica.

5.8. **Requisitos de Implantação**

5.8.1. A Contratada deverá designar um profissional para atuar como Gestor do Contrato de Licenciamento, responsável pela elaboração e acompanhamento de plano de consumo dos benefícios de Software Assurance, decorrentes da aquisição de licenças neste Termo de Referência, garantindo assim o uso eficiente pelo Contratante.

5.8.2. A disponibilização das licenças demandadas deve ser feita de acordo com os prazos definidos no tópico 5.5 (Requisitos Temporais).

5.9. **Requisitos de Garantia**

5.9.1. Os serviços, objeto do presente contrato, terão garantia de funcionamento durante o período de 36 (trinta e seis) meses, a partir da disponibilização das licenças no portal de licenciamento. A CONTRATADA deve informar a data que serão disponibilizadas as licenças no portal.

5.9.2. Correções de problemas e anomalias (bugs) nos softwares, atualizações de versões e releases;

5.9.3. Garantir que novas versões de firmware ou atualizações dos produtos sob contrato de manutenção tenham a perfeita compatibilidade com o ambiente operacional em uso nas instalações computacionais do VALEC.

5.9.4. A CONTRATADA deverá garantir a atualização dos micro-códigos, firmwares, drivers e softwares instalados, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novos releases, a partir do recebimento definitivo pela VALEC, durante o período de garantia.

5.9.5. Caso seja necessário substituir licenças equivalentes durante a vigência do contrato, isso deverá ocorrer sem qualquer ônus para a VALEC.

5.9.6. A garantia deverá contemplar a resolução de qualquer problema nas licenças e serviços descritos neste documento, sem nenhum ônus adicional para a VALEC.

5.9.7. A VALEC somente autorizará que a Contratada faça inventários nos equipamentos quando solicitado formalmente.

5.9.8. A CONTRATADA deverá disponibilizar para a VALEC acesso ao VLSC - Volume Licensing Service Center, serviço disponibilizado pela Microsoft para acompanhamento e uso das licenças e benefícios do contrato.

5.10. **Requisitos de Experiência Profissional**

5.10.1. Não se aplica uma vez que essa contratação visa o fornecimento de subscrições de licenças da Microsoft.

5.11. **Requisitos de Formação da Equipe**

5.11.1. Não se aplica uma vez que essa contratação visa o fornecimento de subscrições de licenças da Microsoft.

5.12. **Requisitos de Metodologia de Trabalho**

5.12.1. Não se aplica uma vez que essa contratação visa o fornecimento de subscrições de licenças da Microsoft.

5.13. **Requisitos de Segurança**

5.13.1. Os serviços em nuvem deverão estar em conformidade com a norma ABNT NBR ISO/IEC 27001:2013;

5.13.2. A CONTRATADA deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela CONTRATANTE de acordo com a PSI - Política de Segurança da Informação da VALEC.

5.13.3. Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato devendo orientar seus empregados nesse sentido.

5.13.4. Não veicular publicidade acerca dos serviços contratados, sem autorização, por escrito, da CONTRATANTE.

5.13.5. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à política de segurança adotada pela CONTRATANTE e as configurações de hardware e de softwares decorrentes e todas as informações do projeto.

5.13.6. A propriedade intelectual e os direitos autorais dos dados e informações armazenados nos bancos de dados da CONTRATANTE, hospedados no CONTRATADO, e qualquer tipo de trabalho relacionado às demandas da CONTRATANTE, serão de sua titularidade, nos termos do art. 4º, da Lei no 9.609/1998.

6. DO ENQUADRAMENTO DO OBJETO

6.1. O objeto da contratação:

6.1.1. É considerado comum, pois possui padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais de mercado;

6.1.2. É de prestação continuada;

6.1.3. Constitui solução de tecnologia da informação;

6.1.4. Dispensa o uso de mão de obra exclusiva;

6.1.5. Tem demanda definida.

7. DO LOCAL DA PRESTAÇÃO DOS SERVIÇOS

7.1. As licenças deverão ser disponibilizadas no portal VLSC, assim como ocorrer a emissão do direito de uso para a Valec Engenharia, Construções e Ferrovias S.A., cuja Sede está localizada no Setor de Autarquias Sul, Quadra 01, Bloco G, Lotes 3 e 5, Asa Sul, Brasília-DF ou em local que venha se subsidiar, dentro do Distrito Federal.

8. CRITÉRIOS DE SUSTENTABILIDADE

8.1. Aplicam-se à presente contratação as disposições constantes na Minuta do Contrato anexo ao Edital.

9. DO REGIME DE EXECUÇÃO

9.1. O regime de execução dos serviços é o de empreitada por preço global.

10. PRAZO DE EXECUÇÃO E VIGÊNCIA DO CONTRATO

10.1. O prazo de vigência e execução do contrato será de 36 (trinta e seis) meses a contar da emissão da Ordem de Serviço.

11. PRAZOS E CONDIÇÕES PARA ENTREGA E RECEBIMENTO DO OBJETO

11.1. As licenças requeridas deverão ser ativadas junto à Microsoft no prazo máximo de 3 dias úteis após emissão da Ordem de Serviço.

11.2. Demais prazos de entrega e recebimento observarão o item 27 e 28 deste termo, no que couber.

12. CRITÉRIO DE JULGAMENTO

12.1. De acordo com o §1º do Art. 1º do Decreto nº 10.024, de 20 de setembro de 2019, esta licitação deve ser realizada na modalidade de PREGÃO na forma ELETRÔNICA, com julgamento pelo critério de Menor Valor por Grupo.

12.2. No critério de julgamento do tipo "menor valor global" é necessária a oferta de preço em todos os itens que compõem o grupo, sendo que os preços ofertados de cada item serão avaliados individualmente, em relação ao respectivo preço estimado, para fins de aceitabilidade da proposta final.

12.3. Da Aplicação do Direito de Preferência e Margens de Preferência:

12.3.1. Nos termos da legislação vigente, quando aplicável, conforme previsão em EDITAL, nas aquisições de bens e serviços de informática e automação definidos pela Lei n.° 8.248, de 1991, será assegurado o direito de preferência conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n.° 7.174, de 2010, e art. 44 e 45 da Lei Complementar n.° 123, de 14 de dezembro de 2006, sendo que as licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência terão prioridade no exercício desse beneficio em relação às médias e às grandes empresas na mesma situação. Destacando-se que a aplicação desse critério e direito ocorre de forma automática no sistema compras governamentais.

13. MODO DE DISPUTA

13.1. O modo de disputa será aberto.

14. HIPÓTESE DE INVERSÃO DE FASES

14.1. Não se aplica a esta contratação.

15. PREÇO REFERENCIAL PARA CONTRATAÇÃO

15.1. Seguem os valores referenciais por itens:

Lote/Grupo	item	SKU	Descrição	Qtde (a)	Valor unitário anual (b)	Valor total anual (c)=(a)x(b)	Valor total para 36 meses = (c)x(3)
1	1	9GS-00495	CISSteDCCore ALNG LicSAPk MVL 2Lic CoreLic	60	*Orçamento Sigiloso*	*Orçamento Sigiloso*	*Orçamento Sigiloso*
	2	7JQ-00341	SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic	12	*Orçamento Sigiloso*	*Orçamento Sigiloso*	*Orçamento Sigiloso*
	3	AAD-33204	M365 E3 Unified ShrdSvr ALNG SubsVL MVL PerUsr	565	*Orçamento Sigiloso*	*Orçamento Sigiloso*	*Orçamento Sigiloso*
	4	1NZ-00004	Defender for Endpoint Server SubVL	48	*Orçamento Sigiloso*	*Orçamento Sigiloso*	*Orçamento Sigiloso*
	5	QLS-00003	Defender for Endpoint SubVL Per User	565	*Orçamento Sigiloso*	*Orçamento Sigiloso*	*Orçamento Sigiloso*
	6	CE6-00004	EntMobandSecE5Full ShrdSvr ALNG SU MVL EntMobandSecE3Full PerUsr	565	*Orçamento Sigiloso*	*Orçamento Sigiloso*	*Orçamento Sigiloso*
	7	NK4-00002	Power-BI PRO	92	*Orçamento Sigiloso*	*Orçamento Sigiloso*	*Orçamento Sigiloso*

15.2. Nos termos do Art. 34 da Lei 13.303/2016, o preço referencial estimado para a contratação será sigiloso, estando exposto no documento SEI 3784783. O preço máximo aceitável será o preço referencial estimado.

15.3. No preço apesentado estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, remuneração da **CONTRATADA**, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação, conforme condições estabelecidas no Edital e na Proposta de Preços da **CONTRATADA.**

16. CRITÉRIO DE ACEITABILIDADE DO PREÇO

16.1. Será aceito o menor valor global observando o valor máximo por item, até o preço referencial estimado conforme item 15 deste termo. Será verificado a exequibilidade nas condições Item 9, do Anexo VII-A, da Instrução Normativa nº. 05/2017 - SEGES/MPDG. "

16.2. O preço máximo aceitável para a contratação é o mesmo do preço referencial da contratação.

17. DA PARTICIPAÇÃO DE CONSÓRCIOS E DE EMPRESAS ME E EPP

17.1. Considerando se tratar de um produto fornecido por diversas empresas, não será permitida a participação de licitantes em consórcio.

17.2. Empresa ME e EPP poderão participar da licitação porém não haverá aplicação de cota exclusiva nos termos do Inciso III do Art. 49 da Lei Complementar 123/2006 e Art. 8º do Decreto 8.538/2015, tendo em vista a natureza do objeto não ser parcelável, conforme justificado no item 4.9 deste Termo de Referência, não tornando vantajoso para administração pública o estabelecimento de cotas para ME e EPP, conforme previsto no inciso II do § único do Art. 10 do Decreto 8.538/2015.

18. DA SUBCONTRATAÇÃO, CESSÃO OU SUB-ROGAÇÃO

18.1. Não será admitida a subcontratação do objeto licitatório.

18.2. Fica vedada a cessão ou sub-rogação do contrato.

19. REQUISITOS DE APRESENTAÇÃO DA PROPOSTAS DE PREÇOS

19.1. A licitante deverá apresentar proposta de preços com os requisitos exigidos no Edital e Modelo constante no ANEXO II – MODELO DE PROPOSTA deste Termo de Referência.

19.2. Devem estar explícitos na proposta o SKU e descritivo das licenças a serem fornecidas bem como quantitativo e demais informações solicitadas no modelo do ANEXO II deste Termo.

19.3. O prazo de validade da proposta é o constante no Edital padrão.

20. REQUISITOS DE CAPACIDADE ECONÔMICO-FINANCEIRA

20.1. I. Certidão negativa de falência, recuperação judicial ou concordata, expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física em data não superior a 120 (cento e vinte) dias.

20.2. II. Balanço Patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta.

20.3. a) O Balanço Patrimonial e Demonstrações Contábeis, quando se tratar de Sociedade Anônima, deverão ser apresentados na forma de publicação em órgão da imprensa público ou privado de acordo com a legislação vigente.

20.4. b) O Balanço Patrimonial e as demonstrações contábeis deverão estar registrados na Junta Comercial ou órgão equivalente, devidamente assinados pelo representante legal da empresa e do contador responsável, (art. 19, § 2º da IN nº 02/2010-MPOG);

20.5. A capacidade financeira da empresa será avaliada conforme a fórmula abaixo que indique a capacidade de crescimento da atividade operacional da empresa maior que zero

20.6. a) Por meio de Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), que deverão ser maiores ou iguais a 1 (um), resultantes da aplicação das fórmulas abaixo, com os valores extraídos de seu balanço patrimonial ou do SICAF:

LG = Ativo Circulante / Passivo Circulante
SG = Ativo Total / (Passivo Circulante + Passivo Não Circulante)
LC = Ativo Circulante / Passivo Circulante

20.7. b) Alternativamente, a proponente deverá comprovar possuir capital social ou comprovação de patrimônio líquido de 10% (dez por cento) do valor estimado da contratação.

21. REQUISITOS DE QUALIFICAÇÃO TÉCNICA

21.1. No processo licitatório, para que possa ser habilitada, a licitante deverá apresentar os seguintes documentos, entre outros que serão exigidos no edital:

21.1.1. Declaração ou Atestado de capacidade técnica para comprovação de execução anterior de atividade pertinente, fornecido por pessoa jurídica de direito público/privado, que comprove ter a licitante fornecido 50% (cinquenta por cento) do quantitativo de licenças de software de ao menos 3 SKUs diferentes indicados neste Termo de Referência.

21.2. No caso de atestados emitidos por empresas privadas, não serão válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa licitante. São consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da empresa licitante, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente ou empresa licitante;

21.3. Em nenhuma circunstância será aceito atestado emitido pela própria licitante.

21.4. As declarações e/ou Atestados de Capacidade Técnico-Operacional deverão conter as seguintes informações:

21.4.1. Identificação do órgão ou empresa emitente com nome ou razão social, CNPJ, endereço, nome da pessoa responsável e função no órgão ou empresa, telefone e e-mail para contato;

21.4.2. Indicação do Contratante de que está atendendo ou foram atendidos os requisitos de qualidade e prazos requeridos (descrição, duração e avaliação dos resultados);

21.4.3. Descrição das principais características dos serviços, comprovando que a licitante executa ou executou o objeto desta licitação.

21.5. Será aceito o somatório de declarações e/ou atestados para fins de comprovação, sendo exigido que esses atestados sejam referentes a contratos executados em períodos concomitantes (conforme Acórdãos de nº 786/2006-P, 170/2007-P, 1.239/2008-P,727/2009-P, 1.231/2012-P e 1.865/2012-P).

21.6. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior (Anexo VII-A IN SEGES/MP nº 05/2017).

21.7. Os atestados de capacidade técnico-operacional deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente (Anexo VII-A IN SEGES/MP nº 05/2017).

21.8. A Valec poderá realizar diligência/visita técnica, a fim de se comprovar a veracidade do (s) Atestado (s) de Capacidade Técnica apresentado (s) pela licitante, quando, poderá ser requerida cópia do (s) contrato (s), nota (s) fiscal (s) ou qualquer outro documento ou informações necessárias à comprovação da legitimidade do (s) atestado (s) apresentado (s).

21.9. Em observância ao item 1.7 do Anexo da Instrução Normativa SGD nº 1/2019, o licitante deverá declarar a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública.

21.10. Após a etapa de habilitação e na data da celebração do contrato será consultado junto ao sítio https://partner.microsoft.com/pt-br/licensing/Parceiros%20LSP a comprovação de que a CONTRATADA esteja apta e autorizada a comercializar licenças por volume EAS demonstrando ainda estar habilitada pela Microsoft para atuar junto a instituições governamentais.

22. FORMAS, CONDIÇÕES E PRAZOS DE PAGAMENTO

22.1. O pagamento será realizado em parcela única anual por um período de 36 meses.

22.2. O pagamento será efetuado por meio de Ordem Bancária (OB), em moeda nacional, em até 30 (trinta) dias, contados a partir da data da apresentação da fatura ou nota fiscal devidamente atestada pelo gestor e ainda o primeiro pagamento condicionado a apresentação do documento comprobatório da Garantia Contratual especificado no Contrato.

22.3. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

22.4. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme previsto neste Termo de Referência.

22.5. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

22.6. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

22.7. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal/Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

22.7.1. o prazo de validade;

22.7.2. a data da emissão;

22.7.3. os dados do contrato e do órgão contratante;

22.7.4. o período de prestação dos serviços;

22.7.5. o valor a pagar; e

22.7.6. eventual destaque do valor de retenções tributárias cabíveis.

22.8. Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

22.8.1. não produziu os resultados acordados;

22.8.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

22.8.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

22.9. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

22.10. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

22.11. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 5(cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

22.12. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

22.13. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

22.14. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

22.15. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

22.16. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da CONTRATANTE.

22.17. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1991,nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

22.18. É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão CONTRATANTE, com fundamento na Lei de Diretrizes Orçamentárias vigente.

22.19. A nota fiscal/fatura deverá ser emitida pela própria CONTRATADA, obrigatoriamente com o número de inscrição do CNPJ, dentro da validade, não se admitindo notas fiscais/faturas emitidas com outro CNPJ, mesmo aqueles de filiais e da matriz.

22.20. Quando aplicável o atendimento do Ajuste do Sistema Nacional de Informações Econômicas e Fiscais (SINIEF) nº. 7, de 30 de setembro de 2005, será necessário que, por ocasião da emissão de suas notas fiscais, a CONTRATADA envie o arquivo digital denominado XML com as respectivas notas ficais eletrônicas emitidas para o seguinte endereço eletrônico: gecon.nfe@valec.gov.br.

22.21. Os contribuintes que não se enquadrarem no estabelecido pelo Ajuste SINIEF nº. 7/2005, por ocasião da assinatura da Ordem de Serviço, deverão elaborar e encaminhar, concomitante, declaração à CONTRATANTE informando essa condição.

22.22. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira diário= 0,00016438, assim apurado:

I = (TX)	I = (6/100)/365	I = 0,00016438 TX = Percentual da taxa anual = 6%

23. DA REVISÃO E DO REAJUSTE DOS PREÇOS

23.1. Os preços são fixos e irreajustáveis.

24. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

24.1. As despesas decorrentes desta contratação, para o exercício de 2021, têm previsão na PL n.º 28/2020 - Projeto de Leo Orçamentária Anual de 2021, com a Lei de Diretrizes Orçamentárias de 2021, Lei nº 14.116 de 31/12/2020, publicada na Edição Diário Oficial da União de 31/12/2020 e com o Plano Plurianual – PPA 2020/2023, Lei nº 13.971 de 27/12/2019, publicada na Edição Diário Oficial da União de 30/12/2019, nos termos do inciso II, do artigo 16, da Lei Complementar nº 101 de 04/05/2000 (Lei de Responsabilidade Fiscal), com especificação abaixo:

- Funcional Programática - 26.126.0032.218T.0000;
- Natureza da Despesa - 3.3.90.40.06 (LOCACAO DE SOFTWARES);
- Fonte de Recursos - 0100;

24.2. O cronograma físico-financeiro será executado anualmente, constará na Nota Técnica 6 SEI 3784783, tendo em vista orçamento sigiloso.

25. DAS OBRIGAÇÕES DA CONTRATANTE E CONTRATADA

25.1. **Deveres e responsabilidades da CONTRATANTE**

25.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos, nos termos do art. 29 da Instrução Normativa ME Nº 01/2019.

25.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;

25.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta

aceita;

25.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;

25.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

25.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

25.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável;

25.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração;

25.1.9. Permitir acesso dos técnicos da CONTRATADA aos locais onde estão instalados os sistema da organização de forma a facilitar as medidas necessárias à prestação do serviço;

25.1.10. A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

25.1.11. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de suas propostas;

25.1.12. Exercer o acompanhamento e a fiscalização dos serviços, pelos fiscais do contrato, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

25.1.13. Notificar à Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

25.1.14. Pagar à Contratada o valor resultante da prestação do serviço de subscrição de licenças, no prazo e condições estabelecidas no Edital e seus anexos;

25.1.15. Promover reunião inicial entre a CONTRATADA e a CONTRATANTE para alinhamento das expectativas;

25.1.16. Fornecer à CONTRATADA as informações necessárias para a plena execução do Contrato;

25.1.17. Detectar eventuais deficiências relacionadas com a execução, sob os aspectos quantitativo e qualitativo, e comunicar as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da CONTRATADA, solicitando imediata interrupção, se for o caso;

25.1.18. Recusar o objeto entregue em desacordo com o contrato de licenciamento;

25.1.19. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante da CONTRATADA;

25.1.20. Proporcionar os meios indispensáveis à boa execução das obrigações contratuais;

25.2. **Deveres e responsabilidades da CONTRATADA**

25.2.1. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;

25.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

25.2.3. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

25.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

25.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação exigidas nos instrumentos que facultaram a contratação, devendo comunicar ao CONTRATANTE a superveniência de fato impeditivo da manutenção dessas condições;

25.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

25.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e

25.2.8. Alocar os recursos necessários para a execução do contrato dentro dos termos pactuados, sem ônus adicionais a CONTRATANTE, além dos estipulados na Proposta Comercial;

25.2.9. Fornecer toda a documentação necessária para Transferência de Conhecimento;

25.2.10. Diante de situações de irregularidades de caráter emergencial, deverá comunicar a CONTRATANTE com os esclarecimentos que julgar necessários e, informações sobre possíveis paralizações de serviços;

25.2.11. Executar os serviços e fornecer as licenças conforme especificações desse Termo de Referência, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer as licenças e serviços, ferramentas e utensílios necessários, na qualidade e quantidade especificada neste Termo de Referência;

25.2.12. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do Contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

25.2.13. Responsabilizar-se pelos vícios e danos decorrentes da execução dos objetos, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar dos pagamentos devidos à(s) Contratada(s), o valor correspondente aos danos sofridos;

25.2.14. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

25.2.15. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

25.2.16. Responder pelos danos causados diretamente ao CONTRATANTE ou a seus aos bens, ou ainda a terceiros, decorrentes de sua culpa ou dolo na execução do contrato;

25.2.17. Respeitar as normas de controle de bens e de fluxo de pessoas nas dependências do CONTRATANTE;

25.2.18. Cumprir os prazos e obrigações estabelecidas no Termo de Referência e Anexos;

25.2.19. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

25.2.20. Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

25.2.21. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do

Contrato;

25.2.22. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação;

25.2.23. Deter instalações, aparelhamento e pessoal técnico adequados e disponíveis para a prestação dos serviços;

25.2.24. Responsabilizar-se integralmente pelo fiel cumprimento dos objetos contratados, prestando todos os esclarecimentos eventualmente solicitados pela contratante, obedecendo aos parâmetros e rotinas estabelecidos de acordo com as recomendações aceitas pela boa técnica, normas e legislação vigentes;

25.2.25. Executar o objeto contratado conforme as condições estipuladas neste Termo de Referência e seus Anexos, e no Contrato;

25.2.26. Indicar formalmente, em 5 (cinco) dias após a assinatura do Contrato, preposto e substituto aptos a representá-la junto a CONTRATANTE, os quais devem responder pela fiel execução dos serviços contratados, orientar a Equipe da CONTRATADA, bem como comparecer às dependências da CONTRATANTE sempre que convocados;

25.2.27. Cuidar para que o preposto mantenha permanente contato com a unidade responsável pela fiscalização do contrato, adotando as providências requeridas à execução dos serviços pelos profissionais, e comande, coordene e controle a execução dos serviços contratados;

25.2.28. Não transferir a outrem, no todo ou em parte, a execução do presente Contrato;

25.2.29. Participar, dentro do período compreendido entre a assinatura do Contrato e o início da prestação dos serviços, de reunião de alinhamento de expectativas contratuais com uma equipe da VALEC que fará a convocação dos representantes da empresa e fornecerá previamente a pauta da reunião;

25.2.30. Atender às solicitações dos membros da Equipe de Gestão do Contrato inerentes às obrigações contratuais e/ou à prestação e/ou à gestão dos serviços;

25.2.31. Comunicar formalmente e imediatamente o Gestor do Contrato todas as ocorrências anormais ou de comprometimento à execução do Contrato, bem como qualquer ocorrência relevante à execução contratual;

25.2.32. Efetuar de imediato o afastamento do atendimento à CONTRATANTE de qualquer empregado cuja atuação, permanência ou comportamento sejam inadequados à execução do Contrato;

25.2.33. Responsabilizar-se por quaisquer encargos, despesas, taxas, inclusive de seguro, decorrentes das operações necessárias à entrega do objeto contratado;

25.2.34. Observar todas as normas de segurança adotadas pela CONTRATANTE, inclusive no que diz respeito às normas referentes ao ambiente informatizado;

25.2.35. Cumprir as disposições do Termo de Compromisso de Sigilo e do Termo de Integridade;

25.2.36. Responsabilizar-se por todos os custos, diretos e indiretos, inclusive de transporte e de pessoal, necessários à adequada prestação dos serviços, em plena conformidade com os termos e especificações, inclusive prazos e horários previstos no Termo de Referência e seus anexos;

25.2.37. Assegurar a disponibilidade, confidencialidade e integridade dos dados, informações e sistemas informatizados, inclusive de todas as suas alterações, manuais, programas fonte e objeto, bases de dados ou outros recursos, pertencentes à CONTRATANTE, armazenados ou residentes na CONTRATADA;

25.2.38. Registrar, tempestivamente, mediante relatório circunstanciado, todos os casos que a eximam de responsabilidade, negligência, mau uso, instalações e outros;

25.2.39. Apresentar fatura no valor autorizado e condições do Contrato, apresentando-a à CONTRATANTE para ateste e pagamento após a autorização de faturamento pelo Gestor do Contrato;

25.2.40. Atender as determinações do Gestor do Contrato inerentes às obrigações contratuais e/ou à prestação e/ou gestão dos serviços;

25.2.41. Fornecer para a CONTRATANTE documentação oficial que comprove o direito de uso das licenças fornecidas junto ao fabricante;

25.2.42. Registrar todas as solicitações feitas pela CONTRATANTE para acompanhamento e controle de fornecimento das subscrições das licenças;

25.2.43. Disponibilizar para download no período contratual todas as atualizações corretivas, evolutivas, de segurança, de funcionalidades, novas versões dos Softwares, de sistemas operacionais garantido pelo licenciamento "SA - Software Assurance".

25.2.44. A CONTRATADA não poderá divulgar projetos, serviços e soluções de TIC da VALEC, nem falar em nome da VALEC em nenhum tipo de mídia sem prévia autorização da VALEC;

25.2.45. Não disponibilizar qualquer informação de propriedade da VALEC, por qualquer meio, a qualquer terceiro e para qualquer finalidade, sem a anuência expressa da VALEC;

25.2.46. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, sendo assim o caso, incluindo a documentação, os modelos de dados e as bases de dados à Administração; e

25.2.47. A Contratada deverá, obrigatoriamente, no momento da assinatura do contrato constar como parceira Microsoft, em consulta ao sítio https://partner.microsoft.com/pt-br/licensing/Parceiros%20LSP que comprove estar apta e autorizada a comercializar licenças por volume EAS demonstrando ainda estar habilitada pela Microsoft para atuar junto a instituições governamentais.

26. DA GARANTIA CONTRATUAL

26.1. Para o fiel cumprimento das obrigações contratuais, o **CONTRATADO** prestará garantia em qualquer das modalidades previstas no artigo 70, § 1º, da Lei nº. 13.303/2016, nos termos do Regulamento Interno de Licitações e Contratos da **CONTRATANTE**, no valor correspondente a 4% (quatro por cento) do valor atualizado do contrato, devendo apresentá-la no prazo de até 10 (dez) dias úteis contados da assinatura da Ordem de Serviço, prorrogáveis por igual período a critério da **CONTRATANTE** e deverá ter validade de pelo menos 90 (noventa) dias após a vigência contratual conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017.

26.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

26.3. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas.

26.4. A garantia inicial será reforçada durante a execução dos serviços contratados, de forma a totalizar sempre os percentuais previstos no item 26.1 do valor vigente do Contrato (preços iniciais mais aditivos e reajustamentos se houver) conforme o caso.

26.4.1. A garantia e seus reforços poderão ser realizados em qualquer das modalidades previstas no artigo 70, §1º, da Lei nº. 13.303 de 2016, a saber:

26.4.2. Caução em dinheiro;

26.4.3. Seguro-garantia;

26.4.4. Fiança bancária.

26.5. No caso de fiança bancária, esta deverá ser a critério da **CONTRATADA**, fornecida por um banco localizado no Brasil, devidamente aptos a operar, registrados em todos os órgãos competentes, inclusive no Banco Central do Brasil, pelo prazo da duração do Contrato, devendo

a **CONTRATADA** providenciar sua prorrogação, por toda a duração do Contrato, independente de notificação da **CONTRATANTE**, sob pena de rescisão contratual ressalvados os casos em que a duração do Contrato for inferior ao prazo acima estipulado, quando deverá a caução ser feita pelo prazo contratual.

26.6. Além disso, a fiança bancária deverá ser devidamente registrada em cartório de registro de títulos e documentos, conforme determinada na Lei nº. 6.015, de 31 de dezembro de 1973, artigo 129, e deverá vir acompanhada de: cópia autenticada do estatuto social do banco; cópia autenticada da ata da assembleia que elegeu a última diretoria do banco; cópia autenticada do instrumento de procuração, em se tratando de procurador do banco e reconhecimento de firmas das assinaturas constantes da carta de fiança. A carta de fiança seguirá o modelo constante no Edital.

26.7. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

26.8. No caso da opção pelo seguro-garantia o mesmo será feito mediante entrega da competente apólice emitida por entidade em funcionamento no País, e credenciada pela Superintendência de Seguros Privados (SUSEP), em nome da **CONTRATANTE**, cobrindo o risco de quebra do contrato, pelo prazo da duração do Contrato, devendo a **CONTRATADA** providenciar sua prorrogação, por toda a duração do Contrato, independente de notificação da **CONTRATANTE**, sob pena de rescisão contratual.

26.9. No caso da opção pelo seguro-garantia, deverá ser adotada a modalidade "Seguro Garantia para Construção, Fornecimento ou Prestação de Serviços" constante do Capítulo II – Condições Especiais das Modalidades – Ramo 0775 do Anexo I da Circular SUSEP n. 477/2013, de forma a assegurar o pagamento de prejuízos causados à Administração decorrentes de culpa ou dolo durante a execução do CONTRATO.

26.10. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados nos subitens da cláusula 26.20, observada a legislação que rege a matéria;

26.11. A garantia em dinheiro deverá ser efetuada em favor da **CONTRATANTE**, em conta específica a ser indicada pela **CONTRATANTE**, com correção monetária.

26.12. No caso de opção por caução em dinheiro, a **CONTRATADA** deverá obrigatoriamente efetuar o depósito na Caixa Econômica Federal (Decreto-Lei nº. 1.737, de 20 de dezembro de 1979, artigo 1º, inciso IV), em conta de caução vinculada à **CONTRATANTE;**

26.13. A garantia prestada pela **CONTRATADA** lhe será restituída ou liberada após o Recebimento Definitivo do(s) serviço(s) e ocorrerá mediante apresentação de certidão de regularidade com o Instituto Nacional do Seguro Social (INSS) relativa à baixa da matrícula do CEI (Cadastro Específico do INSS) e, na hipótese de ter sido realizada em dinheiro, atualizada monetariamente com base na variação do índice da caderneta de poupança.

26.14. A **CONTRATADA** é responsável pelos danos causados diretamente à Administração ou a terceiros, na forma do artigo 77, da Lei nº. 13.303/2016. A **CONTRATADA** é responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do Contrato. A inadimplência da **CONTRATADA** com referência aos encargos trabalhistas, fiscais e comerciais não transfere à **CONTRATANTE** a responsabilidade sobre o seu pagamento, nem poderá onerar objeto do Contrato ou restringir a regularização e o uso das obras e edificações, inclusive perante o registro de imóveis, consoante o disposto no § 1º do artigo 77, da Lei nº. 13.303/2016.

26.15. No caso de consórcio, fica obrigada a empresa líder do consórcio ou seu representante do mesmo a oferecer caução garantia do Contrato.

26.16. O pagamento de todo e qualquer documento de cobrança da **CONTRATADA** somente será efetuado pela **CONTRATANTE** mediante a existência da garantia estabelecida no Contrato.

26.17. Se a garantia for utilizada em pagamento de qualquer obrigação, a **CONTRATADA** deverá fazer a respectiva reposição no prazo de 20 (vinte) dias corridos, contado da data em que for notificada.

26.18. A garantia terá validade durante a execução do Contrato e de 90 dias após após o término da vigência contratual.

26.19. A **CONTRATADA** deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do órgão **CONTRATANTE**, contados da assinatura da Ordem de Serviço comprovante de prestação de garantia, sob pena de aplicação de sanções previstas neste Contrato e no Edital.

26.20. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

26.20.1. prejuízos advindos do não cumprimento do objeto do Contrato;

26.20.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do Contrato;

26.20.3. multas moratórias e punitivas aplicadas pela Administração à **CONTRATADA**; e

26.20.4. obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**, quando couber.

26.21. O garantidor não é parte para figurar em processo administrativo instaurado pelo **CONTRATANTE** com o objetivo de apurar prejuízos e/ou aplicar sanções à **CONTRATADA**;

26.22. A garantia será considerada extinta:

26.22.1. Com a devolução da apólice, fiança bancária ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as Cláusulas do Contrato.

26.22.2. no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

26.23. A **CONTRATADA** autoriza a **CONTRATANTE** a reter, a qualquer tempo, a garantia, na forma prevista no no Edital e no Contrato;

26.24. A **CONTRATANTE** executará a garantia na forma prevista na legislação que rege a matéria;

26.25. A garantia a ser prestada vigorará até o cumprimento integral de todas as obrigações assumidas pelas partes;

26.26. No caso de alteração do valor do contrato, a garantia deverá ser ajustada à nova situação, seguindo os mesmos parâmetros utilizados quando da contratação;

26.27. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a **CONTRATADA** obriga-se a fazer a respectiva reposição no prazo máximo de 15 (quinze) dias úteis, contados da data em que for notificada;

26.28. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas neste instrumento.

26.29. A **CONTRATADA** deverá providenciar a entrega da garantia contratual à **CONTRATANTE**, observando os prazos informados na cláusula 26.1, sendo que o documento deverá ser enviado à área técnica demandante no endereço SAUS, Quadra 1, Bloco "G", Lotes 3 e 5, Asa Sul, Brasília (DF), CEP 70.070-010.

27. MODELO DE EXECUÇÃO DO CONTRATO

27.1. Rotinas de Execução

27.1.1. Em até 05 dias úteis, a partir da assinatura do contrato, deve ser realizada a reunião inicial, na sede da CONTRATANTE ou online, onde a CONTRATADA deverá apresentar formalmente um representante para ser seu Preposto junto à CONTRATANTE e devem ser assinados ainda o termo de

Compromisso e de Sigilo, conforme modelos anexos a este Termo de Referência.

27.1.2. A ordem de serviço será emitida em até 30(trinta) dias da data de assinatura do contrato.

27.1.3. A CONTRATADA terá o prazo de 5 (cinco) dias úteis para realizar a ativação das licenças a partir da entrega da OS.

27.1.4. As licenças solicitadas na OS deverão ser válidas durante o período contratado para execução, garantindo acesso a quaisquer atualizações que venham a ser lançadas nesse período, bem como suporte durante a vigência do contrato.

27.1.5. O pagamento das OS, será realizado em parcela única anual, em até 30 dias corridos, a contar da apresentação da Nota Fiscal/Fatura.

27.1.6. Após a ativação, a CONTRATADA deverá apresentar, no prazo de 2 dias úteis, relatório demonstrativo das licenças ativadas.

27.1.7. A partir do recebimento, a CONTRATANTE terá o prazo de 5 dias úteis para entregar o Termo de Recebimento Provisório - TRP.

27.1.8. Após a entrega do TRP, a CONTRATADA terá o prazo de 10 dias úteis para a entrega do Termo de Recebimento Definitivo – TRD.

27.1.9. A entrega do TRD, autoriza a CONTRATADA a realizar seu faturamento e emitir a Nota Fiscal referente a OS.

27.2. **Quantidade mínima de bens ou serviços para comparação e controle**

27.2.1. Tendo em vista trata-se de solução de mercado, amplamente utilizada, não será necessário quantitativo para comparação e controle.

27.3. **Mecanismos formais de comunicação**

27.3.1. Toda comunicação entre as partes deverá ser realizada por meios oficiais, devendo a CONTRATADA comprometer-se a realizar o seu cadastro junto ao SEI, que deve ser o meio preferencial de comunicação.

27.3.2. Será aceita também a comunicação via E-mail, Ordem de Serviço, Chamamento Técnico, Ofício, entre outros meios oficiais, sempre tendo como prioridade, a comunicação via SEI

27.4. **Manutenção de Sigilo e Normas de Segurança**

27.4.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

27.4.2. O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS III e IV.

28. MODELO DE GESTÃO DO CONTRATO

28.1. **CRITÉRIOS DE ACEITAÇÃO DOS SERVIÇOS**

28.1.1. O recebimento provisório dos serviços prestados será realizado pelo Fiscal Técnico do Contrato, quando da entrega do objeto constante na Ordem de Serviço, da seguinte forma:

28.1.1.1. A Contratada realizará inspeção minuciosa de todos os serviços executados, com a finalidade de verificar a adequação dos serviços e constatar e relacionar as correções que se fizerem necessárias.

28.1.1.2. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

28.1.1.3. No prazo de até 5 (cinco) dias úteis, a partir do recebimento dos documentos da Contratada, cada fiscal ou a equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao Gestor do Contrato para recebimento definitivo.

28.1.1.4. Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do último.

28.1.1.5. Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

28.1.2. No prazo de até 10 (dez) dias úteis a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução do objeto, obedecendo as seguintes diretrizes:

28.1.2.1. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

28.1.2.2. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

28.1.2.3. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

28.1.3. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei nº 10.406, de 2002 e alterações).

28.1.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

28.2. **INSTRUMENTO DE MEDIÇÃO DE RESULTADO**

28.2.1. Todos os serviços fornecidos pela CONTRATADA estarão sujeitos à avaliação e controle de qualidade executados pela VALEC.

28.2.2. O controle de qualidade será executado com base nos parâmetros mínimos estabelecidos no item 28.3 - NÍVEIS DE SERVIÇO.

28.2.3. Durante a prestação dos serviços os Fiscais Técnicos verificarão a atuação dos profissionais da CONTRATADA quanto ao cumprimento da execução do objeto do contrato, dos deveres e responsabilidades da CONTRATADA, item 25.2, considerando a política de segurança da informação da VALEC.

28.3. **NÍVEIS DE SERVIÇO**

28.3.1. Estabelece Acordo de Níveis de Serviço (ANS) de chamados técnicos oriundos de requisições/incidentes ocasionados exclusivamente pela CONTRATADA que possam impactar na prestação dos serviços da solução contratada.

28.3.2. Na abertura de chamados técnicos, serão fornecidas informações de identificação do produto, anormalidade observada, nome do responsável pela solicitação do serviço e severidade do chamado, conforme tabela abaixo:

SEVERIDADE DO CHAMADO				
Severidade	**Descrição**	**Tempo início de atendimento**	**Tempo solução de atendimento**	**Glosa**
Nível 1 (Crítico)	Chamados para solucionar problemas severo que possam afetar gravemente os sistemas em ambiente de produção ou na nuvem como serviço (Saas) que possa torná-los indisponíveis, bem como ocorrer perda de dados de produção e não existir nenhuma alternativa de contorno do problema.	Em até 01 (uma) hora	Em até 03 (três) horas	0,5% sobre o valor da Fatura anual por ocorrência
Nível 2 (Alto)	Chamados para solucionar problemas que causem impacto significativo no desempenho e na qualidade de parte dos serviços. Apesar de não causar interrupção continuada, o serviço em ambiente de produção ou na nuvem como serviço (SaaS) está funcionando com capacidade fortemente reduzida.	Em até 08 (oito) horas	Em até 24 (vinte e quatro) horas	0,2% sobre o valor da Fatura anual por ocorrência
Nível 3 (Médio)	Chamados para solucionar problemas que envolvam a interrupção parcial não-crítica de funcionalidade em ambiente de produção ou na nuvem como serviço (Saas) com impacto de nível médio a baixo na disponibilidade dos serviços. Há prejuízo para algumas operações, mas não compromete todos os serviços.	Em até 24 (vinte e quatro) horas	Em até 72 (setenta e duas) horas	0,02% sobre o valor da Fatura anual por ocorrência

28.3.3. Para efeito dos níveis de severidade serão considerados:

28.3.3.1. Tempo de início de atendimento: Prazo decorrido entre a abertura do chamado efetuada pela equipe técnica da VALEC à CONTRATADA;

28.3.3.2. Tempo de solução de atendimento: Prazo decorrido entre a abertura do chamado efetuada pela equipe técnica do VALEC à CONTRATADA e a efetiva restauração do serviço de subscrição em seu pleno estado de funcionamento.

28.3.4. O atendimento aos chamados de severidade de Nível 1 (Crítico) deverão ocorrer no período 24x7, incluindo período comercial, noturnos, sábados, domingos e feriados.

28.3.5. O atendimento aos chamados de severidade de Nível 2 (Alto), e Nível 3 (Médio) deverão ocorrer em horário comercial.

28.3.6. Por necessidade excepcional de serviço, o CONTRATANTE também poderá solicitar o escalonamento de chamado para níveis superiores de severidade. Nesse caso, a mudança deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

28.3.7. Os chamados, quando possível, poderão ser analisados e solucionados remotamente.

28.3.8. Todos os chamados efetuados receberão código de identificação e serão controlados por sistema de informação da CONTRATADA/FABRICANTE, disponibilizado via web ao qual o CONTRATANTE terá acesso.

28.3.9. O sistema deverá disponibilizar relatório dos chamados técnicos realizados mensalmente.

28.3.10. Chamados fechados sem anuência da VALEC ou sem que os problemas tenham sido de fato resolvidos deverão ser reabertos e os prazos serão contados a partir da abertura original dos chamados, inclusive para efeito de aplicação das sanções previstas.

28.4. **Indicadores de Níveis de Serviços para entrega das licenças:**

INDICADOR DE ATRASO NA ENTREGA DO BEM/SERVIÇO (IAE)

FINALIDADE	Medir o tempo de atraso na entrega das licenças e serviços constantes nas Ordens de Serviço.
META A CUMPRIR	IAE <=0 (A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Serviço dentro do prazo previsto.)
INSTRUMENTO DE MEDIÇAO	Ordem de Serviço, Termo de Recebimento Provisório e Definitivo.
FORMA DE ACOMPANHAMENTO	A avaliação será realizada por meio da verificação da data de entrega constante na ordem de serviço e da data de recebimento provisório das licenças.
PERIODICIDADE	Por ordem de serviço.
MECANISMO DE CÁLCULO (MÉTRICA)	TEX = (DEE - DDE) Onde: TEX = Tempo de execução (quantidade de dias entre o envio da OS e o recebimento provisório). DDE = Data definida para entrega das licenças constante na Ordem deServiço. DEE = Data efetiva da entrega das licenças.
FAIXAS DE AJUSTES NO PAGAMENTO E SANÇOES	Para valores iguais ou inferiores a 0 (zero) - Pagamento integral da Fatura anual; De 1 a 15 (dias de atraso) - Glosa de 5% sobre o valor da Fatura anual; De 16 a 20 (dias de atraso) - Glosa de 10% sobre o valor da Fatura anual; De 21 a 30 (dias de atraso) - Glosa de 15% sobre o valor da Fatura anual; Acima de 30 (dias de atraso) - Será aplicada a multa de 6% sobre o valor do Contrato, sem prejuízo da glosa anterior.

28.5. **Procedimentos de Teste e Inspeção**

28.5.1. Os serviços serão recebidos após a verificação do atendimento dos Níveis Mínimos de Serviços Exigidos.

29. DAS SANÇÕES ADMINISTRATIVAS

29.1. Pelo atraso na execução dos serviços ou pelo não cumprimento de qualquer prazo ou requisito previsto neste Termo de Referência, a não ser por motivo de força maior reconhecido pela Administração, ficará sujeita à multa diária de 0,5% (meio por cento) do valor constante da ordem de serviço em atraso, por dia que ultrapasse o referido prazo, aplicável até o 30° (trigésimo) dia.

29.2. Demais disposições à presente contratação encontram-se constantes na Minuta do Contrato anexo ao Edital.

30. DA ALTERAÇÃO CONTRATUAL

30.1. Aplicam-se à presente contratação as disposições constantes na Minuta do Contrato anexo ao Edital.

31. DA ALTERAÇÃO SUBJETIVA

31.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação

exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

32. DA INEXECUÇÃO E RECISÃO

32.1. Aplicam-se à presente contratação as disposições da cláusula décima nona constante na Minuta do Contrato anexo ao Edital.

33. DA POLÍTICA DE TRANSAÇÕES DE PARTES RELACIONADAS

33.1. A **CONTRATADA** deverá observar a política de transações de partes relacionadas da **CONTRATANTE**, que está disponível no sítio eletrônico da **CONTRATANTE**, no seguinte endereço: https://www.valec.gov.br/download/lei-estatais/Pol%C3%ADtica-de-Transa%C3%A7%C3%B5es-com-Partes-Relacionadas.pdf.

34. DAS DISPOSIÇÕES GERAIS

34.1. Aplicam-se à presente contratação as disposições "Do Comportamento Ético e de Integridade", "Do Antinepotismo", "Da Força Maior", "Das Obrigações Legais e Fiscais", "Dos Direitos de Propriedade Intelectual, Sigilo e Restrições", "Da Renúncia", "Da Publicação" e "Do Foro" da Minuta do Contrato anexo ao Edital, independentemente da ausência de transcrição no presente Termo de Referência.

35. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

35.1. A Equipe de Planejamento da Contratação foi instituída pelo Documento de Oficialização de Demanda 3781122.

35.2. Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

Integrante Requisitante *ROBÉRIO XIMENES SABÓIA* *Gerente de Infraestrutura de TI* SIAPE 1990222	**Integrante Técnico** CLÁUDIO AMORIM DE SOUSA *Gerente de Segurança da Informação* SIAPE 3218987 **Integrante Técnico** JOSE AUGUSTO MEIRA DA ROCHA Analista de Sistemas SIAPE 2340257	**Integrante Administrativo** GICELDA FERREIRA DA SILVA *Assistente Administrativo* SIAPE *1344251*

Autoridade Máxima da Área de TIC
JORGE LUIS DA SILVA LUSTOSA *Superintendente de Tecnologia da Informação* SIAPE 1105206

Brasília, 03 de março de 2021

Documento assinado eletronicamente por **José Augusto Meira da Rocha**, **Integrante Técnico**, em 16/03/2021, às 11:41, conforme horário oficial de Brasília, com fundamento no art. 3º, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Sabóia**, **Integrante Requisitante**, em 16/03/2021, às 11:53, conforme horário oficial de Brasília, com fundamento no art. 3º, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Jorge Luis da Silva Lustosa**, **Superintendente**, em 16/03/2021, às 12:03, conforme horário oficial de Brasília, com fundamento no art. 3º, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Cláudio Amorim de Sousa**, **Integrante Técnico**, em 16/03/2021, às 12:03, conforme horário oficial de Brasília, com fundamento no art. 3º, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Gicelda Ferreira da Silva**, **Integrante Administrativo**, em 16/03/2021, às 15:19, conforme horário oficial de Brasília, com fundamento no art. 3º, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

A autenticidade deste documento pode ser conferida no site https://sei.infraestrutura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3851578** e o código CRC **A2CE7AA3**.

ANEXO I

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

1. SQL SERVER ENTERPRISE

1.1. Controle de redundância;

1.2. Controle de acesso aos dados;

1.3. Garantia de restrições de integridade

1.4. Controle de recuperação a falhas;

1.5. Garantia de acesso imediato aos dados existentes nas bases de dados atuais sem a necessidade de correções e/ou modificações nas aplicações citadas;

1.6. Possibilitar a execução de “backups a frio” e “backups a quente” (completos, diferenciais e transacionais), além da recuperação de dados total, parcial e “point in time”;

1.7. Permitir a replicação/espelhamento de dados entre instâncias de banco de dados diferentes, em servidores iguais ou diferentes;

1.8. Permitir a criação de instâncias de banco de dados em Alta Disponibilidade, a fim de reduzir o Downtime em casos de manutenção ou falha;

1.9. Dispor de suporte técnico especializado, com atendimento em prazo garantido, a fim de se manter os sistemas da Valec com o menor Downtime possível;

1.10. Estar em conformidade com a LGPD;

1.11. Poder rodar em Windows Servers e Linux;

1.12. Operar com dados estruturados e não estruturados;

1.13. Ter documentação sempre atualizada e disponível;

1.14. Permitir encriptação;

1.15. Permitir tabelas temporárias em memória, inclusive com persistência;

1.16. Permitir codificação UTF-8 de caracteres;

1.17. Permitir quantidade ilimitada de cores de CPU;

1.18. Permitir expansão ilimitada de memória;

1.19. Permitir virtualização de dados;

1.20. Possuir facilidades para *tuning* automático do SGBD;

1.21. Permitir classificação de dados;

1.22. Permitir tamanho máximo da base de dados de, pelo menos, 1 PB;

1.23. Possuir ferramentas integradas para acesso, configuração, gerenciamento, administração, monitoração, desenvolvimento de componentes do SGBD e auditoria tanto do servidor quanto dos bancos de dados;

1.24. Permitir segurança a nível de registro;

1.25. Mascaramento de dados;

1.26. Particionamento de tabelas e índices.

2. **A SUITE MICROSOFT 365 E3**

2.1. A suite deve possibilitar e incluir:

2.2. Criar, conectar e permitir colaboração com pessoas, dentro e fora da companhia;

2.3. Permitir que a equipe possa interagir com os membros em qualquer lugar, em dispositivos laptop, móveis, e tablets;

2.4. Instalação dos aplicativos em até 15 dispositivos por usuário incluindo Sistema Operacional Microsoft ou Mac, dispostivos Android, tablets e smartphones;

2.5. Deve possuir as seguintes ferramentas de produção e colaboração operando em aplicativo instalado no computador:

2.6. Publisher, e Access;

2.7. Deve possuir as seguintes ferramentas de produção e colaboração operando em aplicativo instalado no computador, e de forma on-line permitindo a edição para as seguintes ferramentas:

2.8. Word;

2.9. Excel;

2.10. PowerPoint;

2.11. Outlook;

2.12. OneNote;

2.13. Exchange;

2.14. OneDrive;

2.15. Skype for Business;

2.16. Microsoft Teams;

2.17. SharePoint;

2.18. Outlook;

2.19. Yammer;

2.20. Delve;

2.21. Stream;

2.22. Sway;

2.23. Power Apps;

2.24. Power Automate;

2.25. To Do;

2.26. Deve possuir recursos de segurança para gerenciamento e acesso de identidade integrados ao software:

2.27. Microsoft Intune;

2.28. Saúde do dispositivo para Analytics do Windows;

2.29. Microsoft 365 admin center;

2.30. Azure Active Directory Premium plan 1;

2.31. Informação de Proteção contendo:

2.32. Encriptação de mensagem;

2.33. Gerenciamento de acesso;

2.34. Prevenção de perda de dados para e-mail e arquivos;

2.35. Windows Information Protection and Bitlocker;

2.36. Azure Information Protection;

2.37. Da capacidade de armazenamento:

2.38. Espaço de 5TB na nuvem por usuário;

3. **WINDOWS SERVER**

3.1. Compatibilidade com as seguintes tecnologias/soluções:

3.2. Microsoft SQL Server

3.3. Microsoft Sharepoint

3.4. System Center Configuration Manager (SCCM)

3.5. Compor90

3.6. QUANTM

3.7. Assyst

3.8. Deve permitir pelo menos dois acessos simultâneos à Área de Trabalho Remota pelos administradores do Sistema Operacional.

3.9. Ser gerenciável a partir do System Center Configuration Manager (SCCM), que já é utilizado pela VALEC e, dentre outros aspectos, permitir:

3.10. Gerenciamento de servidores e de estações de trabalho

3.11. Inventário de software e de hardware

3.12. Aplicação de patches de segurança

3.13. Deploy de software

3.14. Elaboração de relatórios

3.15. Verificação da aderência de cliente a critérios de *Compliance*

4. ANTIVÍRUS NEXT-GENERATION ANTI-MALWARE

4.1. **Características do agente de proteção contra malwares:**

4.1.1. Pós-execução para verificar e detectar malwares desconhecidos, incluindo zero-days;

4.1.2. O agente deve ser do tipo ligthweight que não degrade a performance do sistema operacional;

4.1.3. O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;

4.1.4. Deverá conter técnicas avançadas de detecção de malwares desconhecidos, utilizando algoritmos de inteligência artificial, como machine learning;

4.1.5. Deve detectar itens maliciosos automaticamente baseado em comportamento (ATP) em memória ou executados, identificando o comportamento malicioso removendo o item malicioso e aplicações potencialmente indesejáveis (PUA);

4.1.6. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

4.1.7. Deverá ser possível recuperar itens da quarentena, que foi considerado falso-positivo;

4.1.8. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

4.1.9. Suportar a instalação dos agentes em máquinas com arquitetura 32-bit e 64-bit, sendo compatível com os sistemas operacionais:

a) Arquitetura Mac OS X 10.10, 10.11, 10.12, 10.13, 10.14, 10.15;

b) Arquitetura Microsoft Windows 8, 8.1 ,10, Windws Server 2012, 2016, 2019

c) Arquitetura Linux CentOS 6/7/8, Ubuntu 19/20, Debian 9/10, Red Hat Enterprise 7, 8.

4.1.10. A instalação da solução de Next Generation Antimalware deve aceitar parâmetros de configuração e distribuição, como instalação silenciosa e definição de diretório de instalação;

4.1.11. Deve permitir a utilização de senha para prevenir a desinstalação do produto nas estações/servidores;

4.1.12. Deve possuir serviço de proteção contra finalização (kill) do processo da ferramenta.

4.1.13. O funcionamento da solução deve operar analisando a execução da ameaça em potencial, nas camadas do Sistema Operacional (O/S), Memória e prevenindo a entrada de códigos maliciosos;

4.1.14. Capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução;

4.1.15. Caso seja identificado um programa malicioso, a sua execução não deve ser permitida;

4.1.16. A solução deve identificar e bloquear a execução de códigos executáveis (binários), scripts ou comandos;

4.1.17. A solução de endpoint deve detectar e prevenir qualquer alteração oriunda de código malicioso ou não-autorizado, em programas que estejam sendo executados em memória;

4.1.18. Deve utilizar a tecnologia de "Machine Learning" para identificar qualquer ameaça nos arquivos potencialmente perigosos;

4.1.19. A análise do malware deve ocorrer em pós-execução, ou seja, o código malicioso no processo de detecção e bloqueio em pós-execução sendo detectadas por comportamento com tecnologia *machine-learning,* não serão aceitas tecnologias que fazem uso de análise de hashing do arquivo por assinaturas;

4.1.20. Identificar ameaças avançadas (ATPs) baseadas em comportamento não devendo utilizar apenas tecnologia baseada em assinaturas (DATs), hashes, detecção por heurística;

4.1.21. Todas as detecções devem ser feitas em tempo real;

4.1.22. Deve permitir controlar dispositivos de armazenamento conectados via USB, permitindo bloquear o acesso ou liberar. Adicionalmente deve ser possível a criação de exceções na política;

4.1.23. O controle do acesso via USB, deve ter a capacidade mínima de controlar os seguintes dispositivos:

a) Dispositivos USB Drive (Pen Drive);

b) Dispositivos virtualizadores como VMWARE, VIRTUALBOX, através de USB Passthrough;

c) Dispositivos portáteis Windows.

4.1.24. A solução não deve possuir tecnologia baseada em assinaturas e hashes para identificação de qualquer ameaça;

4.1.25. Capacidade de extrair mais de 6 milhões de características dos arquivos potencialmente perigosos e aplicar algoritmos de análise para determinar sua intenção;

4.1.26. Prover proteção em tempo real, independente do estado de conexão da máquina, sendo:

a) Online — Com conexão com a Internet;

b) Offline — Sem conexão com a Internet.

4.1.27. Os módulos de proteção de memória e controle de execução devem prevenir técnicas de ataques do tipo:

a) Hijacking;

b) File Injection;

c) File Overflow;

d) In-Memory execution;

e) Exploitation - Stack Pivot, Stack protect, Overwrite Code, RAM Scraping e Malicious Payload;

f) Process Injection — Remote Allocation of Memory, Remote Mapping of Memory, Remote Write to Memory, Remote Write PE to Memory, Remote Overwrite Code, Remote Unmap of Memory, Remote Thread Creation, Remote APC Scheduled;

g) Escalation - LSASS Read e Zero Aliocate.

4.1.28. O módulo de controle e análise de scripts deve ser capaz de analisar no mínimo as seguintes linguagens:

a) PowerShell;

b) Active Scripts — Jscript, WScript, CScript, rmacros, VBA.

4.1.29. O módulo de controle e análise de scripts deve possuir as seguintes ações em caso de violação:

a) Alertar;

b) Bloquear.

4.1.30. Caso ocorra alguma identificação de código malicioso em scripts, a ferramenta deve agir no interpretador e prevenir sua execução imediata;

4.1.31. Deve ser capaz de finalizar processos e sub processos em execução, caso haja a identificação de algum código malicioso sendo executado nos mesmos;

4.1.32. Deve ser capaz de analisar arquivos compactados, como:

a) ZIP;

b) RAR;

c) GZIP;

d) TAR;

e) JAR;

f) WAR.

4.1.33. Deve ser possível a configuração de limite de tamanho e profundidade de compactação para análise de arquivos compactados;

4.1.34. Gerar registro (log) dos eventos de detecção de ameaças em arquivo local, com opção de upload para a console de gerenciamento na nuvem;

4.1.35. Gerar notificações de eventos de ameaças através de alerta via Syslog, por email;

4.1.36. Deve possuir um módulo integrado de Anti-Exploit permitindo identificar e bloquear a execução de Exploits na máquina em memória. Este módulo deve permitir no mínimo a proteção contra ferramentas de injeção de código malicioso, como por exemplo o Shelter, além de detectar e evitar a execução de backdoors;

4.1.37. Deve possuir módulo integrado de bloqueio de Exploits onde não deve ser baseado em assinaturas. Deve ser capaz de bloquear estas ameaças utilizando o próprio engine de inteligência artificial e machine learning;

4.1.38. No modo desconectado, o endpoint deve fazer a detecção e bloqueio usando unicamente o algoritmo matemático. Não serão permitidas soluções hibridas que utilizem assinaturas (DATs), hashes ou consultas na Internet (Cloud Lookups) para a detecção neste cenário;

4.1.39. O endpoint deve ser certificado pela Microsoft como uma ferramenta de AntiVírus, sendo assim, nas plataformas Windows, a ferramenta deve ser identificada como solução de Anti-Virus.

4.2. **Módulo de Análise Forense e detecção e respostas (EDR)**

4.2.1. O módulo de análise forense e detecção e respostas (EDR) deve permitir a monitoração contínua dos eventos, captura e gravação em modo seguro. Este módulo deve permitir analisar o comportamento do malware no endpoint;

4.2.2. Este módulo deve obrigatoriamente estar integrado ao agente do Next-Generation Antimalware, não sendo permitida a adição de agentes adicionais;

4.2.3. O Módulo deve ter a capacidade de coletar informações dos processos em execução da máquina e o motivo para a terminação dos processos;

4.2.4. O módulo deve permitir visualizar através da console web uma linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação;

4.2.5. O módulo deve identificar processos que tenham sido suspensos;

4.2.6. Devem ser fornecidas na console, informações do identificador do processo (Process ID), nome do processo, a linha de comando de execução, o usuário logado que executou o processo, o caminho do executável, e quando disponível o hash MD5 do processo;

4.2.7. O módulo deve reportar eventos maliciosos em memória sendo que devem ser fornecidas no log do evento, os grupos, SID, e quantas vezes o código malicioso tentou executar em memória;

4.2.8. O módulo deve detectar a injeção de ameaças em funções e módulos do programa (aplicativo) executado;

4.2.9. Deve identificar processos suspeitos que executam em localidades não comuns, como diretórios de dados e lixeira;

4.2.10. Deve identificar processos que estabelecem conexões de rede externas e suspeitas (call back);

4.2.11. Quanto as conexões de redes externas e suspeitas devem ser reportadas no log, a origem da conexão, o destino, o tempo de início e término da conexão;

4.2.12. Deve identificar alterações não comuns em áreas do registro da máquina;

4.2.13. Deve monitorar alterações em tarefas agendadas na máquina;

4.2.14. Deve monitorar tentativas de escalação de privilégios;

4.2.15. Deve possuir a capacidade de armazenar toda a informação forense de forma criptografada na própria estação;

4.2.16. Deve permitir realizar um isolamento completo da máquina que foi identificada a ameaça, este isolamento evita a propagação da mesma pela rede;

4.2.17. O agente deve ter a capacidade de fazer este isolamento da máquina por si só, sem necessitar de nenhuma integração com outros softwares ou dispositivos de rede para isso;

4.2.18. Este isolamento pode ser realizado por um tempo específico não inferior a 5 minutos, onde deve ser possível ao administrador fornecer uma chave para realizar a liberação da máquina isolada. Durante o período de isolamento a máquina não consegue realizar nenhuma conexão de rede ficando completamente sem acesso na rede;

4.2.19. Deve ter a capacidade de realizar através da solução o envio do arquivo da sistema de gerenciamento em cloud, para análise posterior;

4.2.20. O módulo de análise forense ou EDR deve possuir a capacidade de identificação automática de comportamentos maliciosos executados no EndPoint através de um conjunto mínimo de 20 regras;

4.2.21. Deve possuir regras para detecção de pelo menos 60 diferentes técnicas de ataques seguindo a classificação e certificação MITRE;

4.2.22. Devem existir pelos menos 10 categorias de regras a serem aplicadas;

4.2.23. Deve ser capaz de permitir a criação de regras de detecção customizáveis utilizando linguagem JSON;

4.2.24. As regras devem apresentar quatro níveis de criticidade: alto, médio, baixo e informativo;

4.2.25. As regras devem identificar pelo menos os seguintes conjuntos de ações:

a) Tentativas de mascarar ou matar os processos no NGAV;

b) Detecção de Fileless Powershell malware;

c) Detecção da execução de comandos maliciosos em Powershell, como comandos que ocultam a execução do Powershell;

d) Invocação maliciosa de JavaScritps com Rundll;

e) Processos de Sistema Operacional iniciados por usuários que não são SYSTEM;

f) Executáveis iniciados do Recycle Bin;

g) Executável criado ou lançado como executável do Windows;

h) Processos do Windows sendo executados ern pastas não padrão;

i) Processos criados com nomes confusos (tentando se passar por processos do Windows);

j) Uso do PSEXEC;

k) Modificação de host files;

l) Tentativa de invocação do Remote Shell;

m) Detecção de executável com múltiplas extensões;

n) Tarefas agendadas suspeitas;

4.2.26. Após identificar estes comportamentos o módulo de EDR deve ter a capacidade de realizar uma ação automática (sem a intervenção do operador), entre as ações automáticas customizadas, devem estar incluídas:

a) Apagar arquivos;

b) Realizar Log Off de todos os usuários, ou usuários remotos, ou usuários interativos;

c) Suspender e terminar processos;

d) Gerar log de aplicação.

4.2.27. Através do dashboard deve ser possível requisitar e fazer download dos logs e evidências causa-raiz, os arquivos maliciosos ou adicionar os mesmos a quarentena global.

4.2.28. Deve ser possível iniciar a execução de scripts em Python na máquina infectada quando se detecte um comportamento malicioso permitindo coletar mais informações forenses como dados do Event Viewer Windows, Registry Hives, Master File Table, Historico do Browser, logs de execução de programas no Windows.

4.3. **Características gerais da console de gerenciamento para endpoints Next-Generation Antimalware do tipo EDR**

4.3.1. Ter capacidade de rastreamento das ações do malware, sendo possível identificar/mapear a ação do ataque, ou seja, onde começou, quais os processos dependentes, ações executadas, através do conceito de telemetria;

4.3.2. Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes;

4.3.3. A solução deve ter características de Endpoint, Detection and Response (EDR);

4.3.4. Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança do tipo SIEM, com opção de configurar qual informação será repassada, como:

a) Log de Auditoria;

b) Dispositivos;

c) Proteção de Memória;

d) Script Control;

e) Ameaças;

f) Classificação de Ameaças;

g) Controle de Aplicação.

4.3.5. A console de monitoração e configuração deverá estar posicionada na estrutura de nuvem através de infraestrutura (SaaS) do fornecedor, sendo uma central única, onde a ferramenta deverá conter recursos para a monitoração e controle da proteção dos dispositivos integrando-se aos agentes;

4.3.6. O fornecedor da console baseada em nuvem deve garantir disponibilidade de pelo menos 99,9% no mês no seu funcionamento;

4.3.7. A console deverá ser do tipo EDR (Endpoint Detection and Response) com característica do tipo telemetria baseado em IA (inteligência artificial) auxiliando na identificação e rastreamento das atividades dos malwares.

4.3.8. A console de gerência deve permitir configurar autenticação em múltiplos fatores;

4.3.9. A console de gerência deve permitir integração de autenticação do tipo SSO (Single-sign-on) através do protocolo idp (identity provider) integrando ao Azure AD;

4.3.10. Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução integrando a árvore do Active Directory ou Azure AD, para possibilitar a segregação de funções;

4.3.11. Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos da árvore do Active Directory;

4.3.12. A console deverá apresentar Dashboard com o resumo dos status de proteção dos endpoints e usuários, bem como correlacionar os alertas de eventos de criticidades alta, média e informacional;

4.3.13. A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;

4.3.14. Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos, usuários ou dispositivos;

4.3.15. A instalação do agente (sensor) deve ser feita através de link por download do pacote disponibilizado na gerência EDR;

4.3.16. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;

4.3.17. Deve permitir criar pacotes de instalação com políticas específicas para distribuição de instalação offline;

4.3.18. Dever permitir a instalação do agente de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft;

4.3.19. Deve ser possível disponibilização de pacote de instalação, configurar parâmetros de linha de comando do tipo arquivo .msi para configurar pelo menos os seguinte item:

a) instalação silenciosa;

4.3.20. O agente deve ser classificado pelo Windows como solução de Antivírus (anti-malware);

4.3.21. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

4.3.22. Possuir módulo na interface web para atualização do produto;

4.3.23. Deve permitir exclusões de escaneamento para um determinado arquivo, processos ou aplicação, tanto a nível geral quanto específico em uma determinada política;

4.3.24. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, politicas e logs;

4.3.25. O módulo de EDR deve ser gerenciado pela mesma console que o endpoint tradicional,

não serão aceitas soluções que trabalham com mais de uma plataforma de gerenciamento.

4.3.26. Pelo módulo de EDR, deve ser possível realizar buscas de itens suspeitos em todos os dispositivos que contenham a solução instalada;

4.3.27. Estas buscas devem permitir pelo menos, mas não limitando-se a: Endereços de IP, arquivos e linhas de comando;

4.3.28. Deve exibir a reputação de um processo para uma análise da legitimidade do mesmo;

4.3.29. Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;

4.3.30. Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;

4.3.31. Utilizar protocolos seguros padrão HTTPS (SSL), com criptografia para comunicação entre console de gerenciamento e clientes gerenciados;

4.3.32. As mensagens de alerta geradas pelo agente (sensor) deverão estar no idioma em Português ou permitir a sua edição;

4.3.33. Permitir a exportação dos relatórios gerenciais para os formatos CSV, HTML ou PDF;

4.3.34. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

4.3.35. Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão do software, eventos recentes e status;

4.3.36. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

a) Detalhar quais hosts de rede (estações, servidores) estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

b) Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

c) Detalhamento dos principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

d) Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

e) Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

f) Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.

4.3.37. A console de gerenciamento deve evidenciar de forma gráfica toda a rastreabilidade de um ataque, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação e identificar informações como a causa raiz de um determinado ataque/infecção;

4.3.38. Devem ser coletadas as atividades de todos artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas/modificadas, conexões de rede realizadas dentre outras, e deve ser possível exportar essas informações;

4.3.39. Deverá ser possível recuperar itens da quarentena, que foi considerado falso-positivo;

4.3.40. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;

4.3.41. O agente antivírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso a web;

4.3.42. Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com uma mesma senha válida para todos os dispositivos;

4.3.43. Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho;

4.3.44. O controle de dispositivos deve ser ao nível de permissão, como somente leitura ou bloqueio;

4.3.45. Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguros, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infravermelho, MTP (Media Transfer Protocol) tais como iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais;

4.3.46. Deve possuir funcionalidades de integração ou monitoramento do firewall local do Windows;

4.3.47. A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetadas para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores;

4.3.48. Deverá possuir interface gráfica web, disponibilizada na lingua Portuguesa e inglesa, prefencialmente no idioma Português.

4.3.49. A Console de administração deve incluir um painel com um resumo visual (Dashboard) em tempo real para verificação do status de segurança;

4.3.50. Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a versão do Antivírus, detalhes de avisos e erros, etc), e classificar os endpoints em conformidade;

4.3.51. Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;

4.3.52. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

a) Nome do dispositivo;

b) Início da proteção;

c) Ultimo usuário logado no dispositivo;

d) Status do escaneamento em tempo real;

e) Último escaneamento realizado;

f) Status de proteção do dispositivo;

g) Grupo a qual o dispositivo faz parte;

4.3.53. Permitir a execução manual de todos estes relatórios, assim como o agendamento e envio automático por e-mail nos formatos CSV, html ou PDF;

4.3.54. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

4.3.55. Deve possibilitar instalação "silenciosa";

4.3.56. Deve permitir o bloqueio por nome de arquivo;

4.3.57. Deve permitir o rastreamento e bloqueio de infecções;

4.3.58. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

4.3.59. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

4.3.60. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

4.3.61. Deve ter a possibilidade de designação do local onde o backup automático será realizado;

4.3.62. Deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;

4.3.63. Deve permitir a deleção dos arquivos quarentenados ou recuperação;

4.3.64. Deve permitir remoção de clientes inativos por determinado período de tempo;

4.3.65. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

4.3.66. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

4.3.67. Possuir gerência centralizada e integrada, a partir de uma única console, para as todas as ferramentas integradas de segurança em estações de trabalho e servidores, de onde seja possível manter a proteção atualizada, gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle

4.3.68. Deve ser possível o gerenciamento de no mínimo 600 máquinas;

4.3.69. Deve permitir o acesso a console de gerenciamento Web, com acesso através de protocolo seguro (HTTPS);

4.3.70. Deve possuir relatórios que permitam no mínimo: ter um sumário das ameaças identificadas, visão geral das ameaças, visão geral dos equipamentos identificando qual a versão do agente está instalada em cada um deles e quanto tempo estão offline;

4.3.71. Deve permitir comunicação segura padrão SSL para conectividade de seus agentes a console de gerenciamento EDR localizada na nuvem;

4.3.72. Deve permitir comunicação segura padrão SSL para conectividade administrativa a console de gerenciamento EDR localizada na nuvem;

4.3.73. Permitir o gerenciamento através de console Web compatível com Mozilla Firefox e Google Chrome;

4.3.74. Deve permitir a definição de níveis diferentes de administração, onde administradores gerenciem, com diferentes níveis de privilégios, grupos de máquinas em diferentes partes do ambiente, havendo, contudo, um grupo de administradores que poderá ter uma visão completa de todo o ambiente instalado;

4.3.75. Deve permitir a atualização automática dos agentes;

4.3.76. Deve suportar a inclusão de certificados digitais para que arquivos assinados com estes certificados estejam dentro de uma lista segura (Safe List) para a execução;

4.3.77. Possuir integração a serviços de diretório LDAP, inclusive Microsoft Active Directory, permitindo a criação de regras para a adição direta das máquinas para os grupos/subgrupos e da console de gerenciamento, da mesma forma que estão nos containers do Active Directory;

4.3.78. Forçar a configuração determinada no servidor para os clientes;

4.3.79. Através da console da ferramenta deve ser exibido à lista dos clientes (estações, servidores) instalado, contendo, no mínimo, as seguintes informações, mesmo com as máquinas desligadas:

a) Nome da máquina;

b) Endereço IP;

c) Versão do sistema operacional (incluindo a versão do Service Pack);

d) MAC Address;

e) Usuário;

f) Versão do endpoint.

4.3.80. Ferramenta deve prover indicadores a partir do seu console único:

a) As 10 máquinas que mais receberam ocorrência de malware;

b) As 10 zonas que mais receberam ocorrência de malware;

c) Os 10 malwares que mais infectaram a rede;

d) Malwares por prioridade;

e) Malwares por classificação;

f) Históricos de infecções em estações/servidores;

g) Históricos de infecções em zonas.

h) Capacidade de exportar os indicadores para o formato CSV e PNG;

4.3.81. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

4.3.82. Possuir módulo que registre em arquivo de log todas as atividades efetuadas pelos administradores permitindo execução de análises em nível de auditoria;

4.3.83. Possuir um painel de controle contendo em tempo real, os indicadores que os administradores da solução julguem necessários para monitorar o ambiente.

5. CASB - CLOUD ACCESS SECURITY BROKER

5.1. **Características da solução CASB para proteção contra ameaças de malwares, vazamento de dados (DLP), e Auditoria - na nuvem (SaaS)**

5.1.1. Identificar os dados que estão sendo compartilhados na conta do Office365, e modificar as permissões de compartilhamento para remover qualquer exposição pública;

5.1.2. Detecção automática e granular de conteúdo sensível para upload a partir de aplicativos de e-mail, compartilhamento de arquivos (file-sharing), repositório de dados;

5.1.3. Bloquear risco elevado de compartilhamento de confidencialidade de dados para rede pública, usuários externos, para a organização, e aplicativos em nuvem não-sancionadas;

5.1.4. Deve prevenir vazamento de dados (DLP), com monitoramento real, lendo o conteúdo do documento, identificando “dados sensíveis”;

5.1.5. Deve possuir módulo DLP integrado baseado em machine-learning, para:

I - políticas pré-definidas;

II - customização de expressões regulares;

III - customização de dicionários;

IV - prevenção de exportação de dados de contas corporativas para contas pessoais;

V - monitoramento de atividades de aplicativos em nuvem sancionadas e não-sancionada;

5.1.6. Deve possuir módulo DLP integrado baseado em m

5.1.7. Deve possuir políticas para bloqueio de arquivos confidenciais de aplicativos corporativas sancionadas para aplicativos não-sancionadas da nuvem;

5.1.8. Deve possuir políticas para filtro de aplicativos em nuvem não-sancionados de uso pessoal de contas na nuvem baseado em critérios de ranking;

5.1.9. Deve descobrir e categorizar os aplicativos em nuvem usadas pelos dispositivos gerenciados e não-gerenciados;

5.1.10. Deve analisar os aplicativos em nuvem utilizadas pelos dispositivos gerenciados e não-gerenciados (BYOD) a fim de identificar na console CASB os aplicativos sancionados pela PSI da VALEC e não-sancionados, conceito *Shadow IT;*

5.1.11. Deve possuir classificação de segurança para aplicativos em nuvem sancionadas e não-sancionadas (*Shadown IT*) para os padrões de conformidade internacionais (LGPD, GDPR, "DADOS SENSÍVEIS", FERPA, and GLBA);

5.1.12. Deve gerar relatórios abrangentes com resumos executivos juntamente com uma lista de serviços descobertos e recomendações (por exemplo, classificação geral de risco corporativo);

5.1.13. Deve identificar os principais usuários de aplicativos de nuvem que ofereçam risco elevado e resolva atividades de risco por meio de treinamento ou intervenção

5.1.14. Deve permitir comparação de apps com funcionalidades similares lado-a-lado e consolidar a opção mais segura;

5.1.15. Geração de relatórios executivos de forma sumarizada contendo lista de serviços (app's sancionadas, não-sancionadas, auditoria) descobertos e recomendações de risco;

5.1.16. Atualização automática e contínua do catálogo de aplicativos em nuvem e classificação do risco do uso;

5.1.17. Incluir quantidade de usuários, ações, volume de tráfego, e tempo de uso de cada aplicação na nuvem;

5.1.18. Possibilitar a customização do painel dashboard para visualização de atividades, usuários e dispositivos com granularidades suficientes;

5.1.19. Possibilitar visualização em painel dashboard das aplicações na nuvem mais utilizadas, quais dispositivos BYOD e usuários utilizam

5.1.20. Restringir usuários para acesso a apps da nuvem que contenham vulnerabilidades;

5.1.21. Capacidade de bloquear, redirecionar e alertar sobre violações de políticas, permitindo que as organizações restrinjam os serviços de nuvem não aprovados, permitindo o acesso àqueles que atendem;

5.1.22. Possibilitar autenticação de usuário a solução CASB, havendo integração desta à identidade do usuário de domínio na nuvem através do Azure Active Directory (VALEC) sendo que a solução CASB atuará como autenticador do tipo SSO (single sign-on) utilizando protocolo IdP, através da interoperabilidade SAML 2.0 (Security Assertion Markup Language).

5.1.23. Deve fazer update da database de aplicativos em nuvem com as informações de risco;

5.1.24. Deve ter habilidade de bloquear, redirecionar e alertar política violada possibilitando ou não o acesso, considerando a PSI da VALEC;

5.1.25. Deve possuir análise de risco baseado em regras Data-Loss Prevention (DLP) baseadas na Lei Geral de Proteção de Dados Pessoais (LGPD) e na lei europeia de proteção de dados pessoais (GDPR);

5.1.26. Deve possuir análise de risco baseado em atributos da LGPD - "dados sensíveis" para aplicativos em nuvem (cloud app);

5.1.27. A partir do Dashboard a solução deve propiciar relatórios de visibilidade de aplicativos em nuvem para monitorar se o uso do aplicativo em nuvem (cloud add) está de acordo com as regulamentações da LGPD;

5.1.28. Realizar avaliações de impacto do fornecedor de aplicativos na nuvem e bloquear o uso de aplicativos não compatíveis com a LGPD;

5.1.29. Deve possibilitar aplicação de controles de acesso para políticas baseadas em localidade geográfica;

5.1.30. Classificação de "dados sensíveis" automatizada do conteúdo que está sendo carregado e armazenado em aplicativos e serviços em nuvem;

5.1.31. Correção de exposições de risco e aplicação de política contínua para evitar vazamento de conteúdo de "dados sensíveis" na nuvem (DLP).

5.1.32. Deve possibilitar criptografia de dados pessoais, em aplicativos em nuvem (cloud app) e serviços, para "dados sensíveis";

5.1.33. Possibilitar resposta rápida a incidentes para facilitar os requisitos de notificação de violação de dados;

5.1.34. Possuir controles de acesso baseados em funções e relatórios personalizados para fornecer acesso correto e visibilidade exigidos por um encarregado de dados (LGPD);

5.1.35. Identificar novas instâncias de aplicativos em nuvem dos provedores AWS, Google Cloud, Azure e outros, para aplicativos em nuvem adquiridos fora da TI da VALEC;

5.1.36. Possuir capacidade de descobrir todas as contas em nuvem usadas na rede corporativa, incluindo contas pessoais.

5.1.37. Possuir capacidade de processar atividades detalhadas do usuário de interfaces de API para aplicativos e serviços em nuvem sancionados, como Office365, Amazon Web Services e Google G-Suite;

5.1.38. Gerar relatórios personalizados que atendam aos requisitos e cronogramas organizacionais;

5.1.39. Extrair análise detalhada do tráfego HTTPS em tempo real para identificar a atividade do usuário em uma ampla gama de aplicativos e serviços em nuvem;

5.1.40. Processar dados de registro consolidados com funções de pesquisa e filtragem intuitivas para identificar e explorar incidentes de interesse, como controle de conta, tentativas de transferência não-autorizada de dados (exfiltration) e destruição de dados.

5.1.41. Detecção automática e granular de políticas para conteúdo de "dados sensíveis" carregados para ou criado aplicativos na nuvem como compartilhamento de arquivos (file-sharing), repositório de dados, e chat;

5.1.42. Possibilitar o bloqueio de compartilhamento de dados confidenciais, classificando como risco elevado para: meio público, usuários externos, para toda a organização, e contas não-sancionadas;

5.1.43. Deve possuir filtro DLP baseado em machine-learning com conteúdo pré-definido e classes de risco de dados, termos pré-definidos, customização de expressões regulares, e dicionários.

5.1.44. Integração com o Azure Active Directory e serviços SSO para associação de atribuição de usuários e grupos as políticas;

5.1.45. Identificar vazamento de dados (DLP) e violação de “dados sensíveis” nas suítes de escritório Office 365 e suas Apps: OneDrive, Outlook/email, Sites, Yammer, Teams, and Groups, e GSuite e suas Apps: Drive, Gmail, Calendar, Hangouts, Sites, Vault, Contacts, e Admin.

5.1.46. Deve possuir módulo de prevenção de download de conteúdo de arquivos associados a aplicativos em nuvem corporativos sancionados, ex. Office 365, GSuite, para upload em contas pessoais de aplicativos em nuvem não-sancionados, ex. One Drive, Dropbox, Google Drive, alertando o administrador;

5.1.47. Possuir modo de proxy de encaminhamento para monitorar atividades na nuvem sancionadas e não-sancionadas para detectar padrões de downloads a partir de conta Office 365 corporativa, seguido de upload para aplicativos em nuvem não-sancionados ex. Dropbox, Google Drive, alertando o administrador;

5.1.48. Possuir módulo de proteção contra conteúdo malicioso de entrar no ambiente corporativo a partir de outros aplicativos em nuvem;

5.1.49. Deve detectar, bloquear, reportar, e prevenir a proliferação de arquivos maliciosos;

5.1.50. Inspecionar as apps da suíte Office 365 e comunicação das ferramentas de colaboração, Teams, SharePoint contra ações de malwares e atividades de alto risco;

5.1.51. Detectar, bloquear, alertar, e prevenir proliferação de arquivos maliciosos para os aplicativos em nuvem, e dados estruturados;

5.1.52. Detectar ameaças do tipo zero-day incorporadas a contas de aplicativos em nuvem sancionadas;

5.1.53. Possuir sandbox na nuvem para analisar arquivos desconhecidos e detectar o malware antes de fazer o upload dele no ambiente de nuvem corporativo;

5.1.54. Identificar transações de risco baseado em padrões de comportamento do usuário, através do acesso de conteúdo de informações sensíveis, ou através de customização para definição de transações.

5.1.55. O módulo de proteção ativa deve verificar conteúdo via API através de solução de Antivírus Next-Generation para identificação de ameaças avançadas, independente da origem e conteúdo de dispositivos gerenciados ou não-gerenciados, aplicativos externos em nuvem ou conta.

5.1.56. Identificar e colocar em quarentena malwares e macros VB (incluindo sua comunicação com comandos e servidores de controle);

5.1.57. Ter suporte de proxy de encaminhamento para monitorar e controlar as atividades do usuário e acesso a dados através de aplicações nativas por meio de aplicativos de terminal nativos para aplicativos em nuvem;

5.1.58. Deve correlacionar as atividades de anomalias de malwares com o risco associado, emitindo alerta de bloqueio, quarentena, para o malware, informando o dispositivo e usuário relacionado;

5.1.59. Deve possuir Muti-Fator de Autenticação;

5.1.60. Deve possuir autenticação do tipo SSO (Single Sign-On) possibilitando redirecionamento de autenticação utilizando o protocol IdP integrando a entidades terceiras que utilizam o protocolo SAML 2.0;

5.1.61. Possuir API nativa para integração com plataformas do tipo SIEM (security information and event management);

5.1.62. O fornecedor da console CASB baseada em nuvem deve garantir disponibilidade de pelo menos 99,9% no mês no seu funcionamento;

5.2. **Da integração das solução CASB com a solução de Endpoint Next-Generation Antivirus são obrigatórios os seguintes recursos:**

5.2.1. A solução Next-Generation Antivirus, integra-se a solução CASB sendo possível bloquear o acesso a URL's ou endereços através do CASB;

5.2.2. Bloqueio a determinadas URL's diretamente no dispositivo mesmo fora da organização, não sendo necessário aplicar o bloqueio em ativos como firewalls, proxies, e em nível de DNS;

5.2.3. Aplicação de regras condicionais para o CASB baseadas na verificação do agente de endppoint;

5.2.4. A verificação de propensos arquivos infectados ao qual o usuário faria o (upload) passando pelo MCAS, não necessita de verificação pelo MCAS, poupando recursos, devido ao endpoint já possuir o agente Antivirus instalado; (zero-trust)

5.2.5. O CASB deve usar as informações de tráfego coletadas pelo agente de endpoint de Antivírus sobre os aplicativos e serviços em nuvem acessados a partir de dispositivos Windows 10 gerenciados pela TI. A integração nativa permite que execução do Cloud Discovery em qualquer dispositivo da rede corporativa, usando Wi-Fi público, em roaming e por acesso remoto. Deve também permite a investigação baseada no dispositivo;

5.2.6. O deve coletar os logs dos endpoints. A integração nativa traz a vantagem quanto a descoberta de Shadow IT em dispositivos Windows em sua rede;

5.2.7. Os aplicativos marcados como não-sancionados no CASB são automaticamente sincronizados no endpoint de Antivírus. Mais especificamente, os domínios usados por esses aplicativos não-sancionados são propagados para dispositivos de endpoint para serem bloqueados pelo endpoint Antivirus dentro do SLA de proteção de rede;

5.2.8. Integração do CASB entre o serviço de identidade do Microsoft Azure AD (Azure AD Identity Protection).

5.3. **Da integração da solução CASB com a suite de escritório Office 365, são obrigatórias as seguintes remediações em eventos de DLP e segurança:**

5.3.1. Excluir um arquivo e pasta violado para a lixeira do administrador;

5.3.2. Colocar o arquivo e pasta violada na quarentena do administrador;

5.3.3. Colocar o usuário em quarentena;

5.3.4. Remover o colaborador específico;

5.3.5. Remover permissão específica de um arquivo ou pasta do Office 365, revertendo a permissão na pasta herdada (pai);

5.3.6. Habilitar eventos de auditoria do Exchange no Office 365, quando um usuário for definido com privilégios administrativos possibilitando a visualização de alertas no solução CASB;

5.3.7. Rastrear atividades de usuário no Power-BI;

5.4. **Da integração da solução de CASB com o Azure Active Directory, são obrigatórias as seguintes ações:**

5.4.1. Notificar o usuário através de alerta via Azure AD;

5.4.2. Requere que o usuário faça login novamente via Azure AD;

5.4.3. Suspender automaticamente o usuário via Azure AD;

5.4.4. Capacidade de integrar-se ao log de eventos de identidade do Azure AD Identity Protection;

5.4.5. Mostra alertas de vazamento de credenciais;

5.4.6. Agregar várias detecções de tentativas de falhas de login que não foram realizados pelo usuário;

5.4.7. Sincronismo de logs de eventos de segurança do Azure AD Identity Protection;

5.4.8. Integração nativa com a "Proteção de Identidade" do Azure Active Directory (Azure Active Directory Identity Protection) possibilitando identificar análise de comportamento.

ANEXO II

Modelo de Proposta de Preço

À Valec Engenharia, Construções e Ferrovias S.A., Pregão Eletrônico n.º_____

Licitante:_____ CNPJ:_____

Endereço:_____

Telefone: (__)_____E-mail:_____

Representante Legal:_____

Nacionalidade:_____Estado Civil:_____

Profissão:_____Função na Sociedade:_____

RG:_____CPF:_____

Estabelecimentos vinculados à execução contratual (Matriz/Filial):

Razão Social:_____CNPJ:_____

Endereço:_____

Razão Social:_____CNPJ:_____

Endereço:_____

Lote/Grupo	item	SKU	Descrição	Qtde (a)	Valor unitário anual (b)	Valor total anual (c)=(a)x(b)	Valor total para 36 meses = (c)x(3)
1	1	9GS-00495	CISSteDCCore ALNG LicSAPk MVL 2Lic CoreLic	60			
	2	7JQ-00341	SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic	12			
	3	AAD-33204	M365 E3 Unified ShrdSvr ALNG SubsVL MVL PerUsr	565			
	4	1NZ-00004	Defender for Endpoint Server SubVL	48			
	5	QLS-00003	Defender for Endpoint SubVL Per User	565			
	6	CE6-00004	EntMobandSecE5Full ShrdSvr ALNG SU MVL EntMobandSecE3Full PerUsr	565			
	7	NK4-00002	Power-BI PRO	92			

Descrição das características detalhadas do I:

O Licitante _____ Declara ter ciência e aceitar as condições apresentadas, propondo, em acordo com elas, o valor global de R$ _____ (_____), observados os valores unitários cotados na planilha acima.

Declaramos, outrossim, que o valor proposto inclui todas as despesas e custos, diretos e indiretos (inclusive tributos e/ou impostos, remuneração da **CONTRATADA**, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros), necessários ao cumprimento integral do objeto.

Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no TERMO DE REFERÊNCIA.

Cumprimos todas as exigências do edital quanto a elaboração da proposta comercial de licitação.

Por fim, a Licitante _____ informa que a validade da proposta é de __ (_____) dias.

_____, ___ de _____ de 2021

(Representante Legal da Licitante)

ANEXO III

TERMO DE COMPROMISSO

O <*NOME DO ÓRGÃO*>, sediado em <*ENDEREÇO*>, CNPJ n.° <*CNPJ*>, doravante denominado CONTRATANTE, e, de outro lado, a <*NOME DA EMPRESA*>, sediada em <*ENDEREÇO*>, CNPJ n.° <*CNPJ*>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE SIGILO E CONFIDENCIALIDADE, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 4.553 de 27/12/2002 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de idéias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da eqüidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOs e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

_____, _____ de _____ de 20____

De Acordo,

CONTRATANTE	**CONTRATADA**
_____ ***<Nome>*** **Matrícula: *<Matr.>***	_____ ***<Nome>*** ***<Qualificação>***
Testemunhas	
Testemunha 1 _____ ***<Nome>*** ***<Qualificação>***	**Testemunha 2** _____ ***<Nome>*** ***<Qualificação>***

ANEXO IV
TERMO DE CIÊNCIA

IDENTIFICAÇÃO DO CONTRATO			
Contrato Nº			
Objeto:			
Gestor do Contrato:		Matricula:	
Contratante (Órgão):			
Contratada:		CNPJ	
Preposto da Contratada:		CPF	

Por este instrumento, os funcionários abaixo assinados declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes na Contratante.

Brasília, _____ de_____ _____ de 20_____.

CIÊNCIA	
CONTRATADA	
_____ <Nome> Mat.:	_____ <Nome> Mat.:
_____ <Nome> Mat.:	_____ <Nome> Mat.:

ANEXO V

MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO Nº xxx/2021

PROCESSO:					
CONTRATO Nº:					
CONTRATANTE: VALEC Engenharia, Construções e Ferrovias S.A.			**ORDEM DE SERVIÇO**		**Número**
ESCRITÓRIO BRASÍLIA					
CONTRATADA:			DATA DE EMISSÃO / /		
CNPJ:					
FICA AUTORIZADA A FORNECER O MATERIAL ABAIXO NAS CONFIÇÕES ESTIPULADAS A SEGUIR:					
ITEM	QTDE	UNIDADE	DESCRIÇÃO DO MATERIAL	PREÇO UNITÁRIO (R$)	PREÇO TOTAL(R$)
		UN.			
Valor desta O.S.: R$ xxx.xxx,xx <Valor por extenso>					
A Contratante, por meio dos seus Fiscais xxxxxx, requer à Contratada a prestação dos serviços objeto do contrato em epígrafe, conforme especificações e condições acordadas. Os serviços deverão iniciar-se até o dia xxxx.					
5.5. O PRESENTE DOCUMENTO REPRESENTA PARA TODOS OS EFEITOS, UMA ADJUCAÇÃO DO CONTRATO DE SERVIÇO DE SUBSCRIÇÃO DE LICENÇAS MICROSOFT.					
xxxxxxx xxxxx xxxxx Fiscal Técnico			**xxxxxxx xxxxx xxxxx** Fiscal Requisitante	**xxxxxxx xxxxx xxxxx** Gestor do Contrato	
ACEITE DO FORNECEDOR					

Recebi, em ___/___/____, a presente Ordem de Serviço, obrigando-me desde já a realizar os serviços dela, no prazo e valor acima indicado.

DATA: / /	_____ Nome, Assinatura do Responsável Legal pela Contratada, RG e CPF

ANEXO VI

MINUTA TERMO DE RECEBIMENTO PROVISÓRIO

Processo nº:	
Objeto:	Vigência:
Contratada:	CNPJ:
Nº da NE:	
Valor da NE:	
Desconto/glosa/ajuste de pagamento:	
Data prevista para entrega/conclusão do serviço:	Data da efetiva entrega/conclusão do serviço:

Aos xxxx dias do mês xxxx de xxxx, com fundamento na Instrução Normativa SLTI/MP nº 04/2014, e após acompanhamento, fiscalização e verificação dos serviços xxxxxxx, prestados pela Contratada em epígrafe, realizados no período de xxx a xxx, certifico a conformidade dos mesmos com os temos contratuais.

Informo que foram verificadas as hipóteses de glosa, resultando no seguinte xxxx.

O objeto contratual foi executado de forma satisfatória. Foi executado (detalhar o que foi executado, do ponto de vista técnico da TI) no período de (informar datas), razão pela qual lavro este TERMO DE RECEBIMENTO PROVISÓRIO, para os fins legais e para efeitos de pagamento.

_____,_____de_____de 2021.

Fiscal Técnico

_____

Fiscal Requisitante

_____

Ciente em __/__/____.

Representante da Contratada

_____

ANEXO VII

MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

Processo nº:	
Objeto:	Vigência:
Contratada:	CNPJ:
Nº da NE:	
Valor da NE:	
Desconto/glosa/ajuste de pagamento:	
Data prevista para entrega/conclusão do serviço:	Data da efetiva entrega/conclusão do serviço:

Aos xxxx dias do mês xxxx de xxxx, com fundamento na Instrução Normativa SLTI/MP nº 01/2019, e após verificação dos serviços xxxxxxx, prestados pela Contratada em epígrafe, realizados no período de xxx a xxx, ratificamos a conformidade dos mesmos com os temos contratuais.

Informo que foram verificadas as hipóteses de glosa, resultando no seguinte xxxx.

O objeto contratual foi executado de forma satisfatória. Foi executado (detalhar o que foi executado, do ponto de vista do negócio e do contrato) no período de (informar datas), razão pela lavramos este TERMO DE RECEBIMENTO DEFINITIVO, para os fins legais e para efeitos de pagamento.

_____,_____de_____de 2021.

_____

Fiscal Requisitante

_____

Gestor

SAUS Quadra 01, Bloco G, Lotes 3 e 5 - Bairro ASA SUL
Brasília/DF, CEP 70070010
Telefone: 2029-6100 - www.valec.gov.br