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

Estudo Técnico Preliminar da Contratação/SUPTI-VALEC/DIRAF-VALEC-VALEC

Brasília, 06 de fevereiro de 2021.

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
06/02/2020	1.0	Finalização da primeira versão do documento	Cláudio Amorim de Sousa
20/02/2020	1.1	Revisão prévia de envio ao setor de licitações	Jorge Luis da Silva Lustosa

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1. INTRODUÇÃO

1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda SEI 3781122, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. Durante o Estudo Técnico Preliminar, diversos aspectos devem ser levantados para que os gestores certifiquem-se de que existe uma necessidade de negócio claramente definida, há condições de atendê-la, os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente.

1.3. O objeto do estudo é a contratação de solução de segurança para proteção de ameaças digitais ***Endpoint Next-Generation Anti-malware*** que atendam de forma ampla às necessidades da Valec Engenharia, Construções e Ferrovias S.A.

2. MOTIVAÇÃO/JUSTIFICATIVA

2.1. A crescente difusão de ameaças tecnológicas tais como vírus de computador e outros malwares, podem causar diversos prejuízos financeiros e administrativos irreparáveis à VALEC. Portanto, faz-se necessária a proteção dos ativos da informação da VALEC, bem mais valioso da estatal.

2.2. Dentre as ameaças mais recentes temos o Ransomware, um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para que seja possível restabelecer o acesso aos dados pelo usuário. O ransomware pode se propagar de diversas formas, embora as mais comuns sejam através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link ou explorando vulnerabilidades em sistemas operacionais, e sofwares que não tenham recebido as devidas atualizações de segurança.

2.3. Conforme a cartilha de segurança para internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.BR.

> *“para manter o seu computador livre da ação dos códigos maliciosos existe um conjunto de medidas preventivas que você precisa adotar. Essas medidas incluem manter os programas instalados com as versões mais recentes e com todas as atualizações disponíveis aplicadas e usar mecanismos de segurança, como antimalware e firewall pessoal”.*

2.4. A partir revisão da Política de Segurança da Informação proposta pela Gerência de Segurança da Informação GSINF/SUPTI/DIRAF, sendo aprovada pelo Conselho da Administração (CONSAD) em 13/01/2021, destaca-se no subitens 1.3.2 e 1.3.3. do item "1. Das Disposições Preliminares":

> *"1.3.2 Esta Política deve ser, obrigatoriamente, observada nas definições de regras operacionais, nas normas e nos procedimentos no âmbito da VALEC.*
>
> *1.3.3. Estabelece mecanismos e controles para garantir a efetiva proteção dos dados, das informações e dos conhecimentos gerados e visa minimizar os riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações da empresa."*

2.5. O uso de software de antivírus é um mecanismo que visa proteger os usuários da VALEC contra ataques malwares, que são "programas" especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela auto-execução de mídias removíveis infectadas, como *pen-drives*;
- pelo acesso a páginas *Web* maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web* ou diretamente de outros computadores (através do compartilhamento de recursos).

2.6. Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

2.7. Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam."* Fonte: https://cartilha.cert.br/malware/ [Acesso em 22/01/2021]

2.8. Portanto, faz-se indispensável a aquisição de software com tecnologia de detecção e proteção baseada em comportamento - Next-Generation Anti-malware, de forma a coibir a contaminação dos serviços e sistemas informatizados e estações de trabalho por programas ou atividades digitais maliciosas, contribuindo para a garantia do nível mínimo adequado e desejado de proteção dos dados e informações da VALEC. É fundamental ter mecanismos tecnológicos que garantam a segurança dos dados e informações de propriedade no âmbito da VALEC.

2.9. Para a ferramenta centralizada, a console de gerência "*Endpoint Detection Response*" (EDR), permitirá à equipe de segurança o monitoramento das ações executadas pelo propenso vírus (telemetria), o status das ameaças que foram detectadas para cada estação, o status de proteção dos endpoint através dos agentes, visibilidade geral de proteção dos endpoint com classificação de severidade das ameaças.

2.10. Em suma a aquisição de software de proteção *Endpoint Next-Generation* Anti-malware propiciará:

I - Proteção ativa para Endpoint contra ações de malwares utilizando tecnologia de proteção a ameaças avançadas (ATP) - Endpoint Next-Generation (NGAV) baseada em comportamento (*machine learning).*

II - Proteção aos ativos da informação da VALEC contra ameaças anti-malware;

III - Gerenciamento dos Endpoints Next-Gen Anti-malware através da console EDR posicionada na nuvem (SaaS) com SLA de funcionamento do fornecedor/fabricante de 99,9%;

IV - Consonância com a PSI da VALEC e IN 01 2019 da SGD.

V - Proteção a infraestrutura de segurança dos dados armazenados na instituição e carregados na nuvem provendo confidencialidade, integridade e disponibilidade das informações trafegadas e armazenadas nas estações de trabalho e servidores nos mais diversos sistemas corporativos da VALEC.

2.10.1. **Do contrato atual**

2.10.1.1. O contrato atual para solução de endpoint Anti-malware, estabelecido entre VALEC e SWTI Tecnologia (36/2018), que utilizava o software da fabricante Symantec - SEP (Symantec Endpoint Protection), teve vigência até 18 de janeiro de 2021, não sendo vantajoso para a empresa sua renovação, por se tratar de tecnologia de proteção ultrapassa e baseada em assinatura, desatualizada e ineficaz contra novas ameaças que praticamente paralizaram o governo no semestre passado, conforme publicação (3790110) . Cabe observar também que desde Julho de 2020 esta SUPTI já vem alertando para o fato que se trata de tecnologia defasada e sobre falta da vantajosidade do contrato conforme despacho 74 (2614566) do processo 51402.100283/2020-59 onde a DIRAF, orienta sobre a análise dos contratos vigentes. Desde então vem estudando soluções que possam melhorar o nível de segurança e a solução utilizada com sucesso no mercado tem sido a tecnologia baseada em comportamento (machine-learning) Next-Generation Anti-Malware que será detalhada mais adiante no item 3.1.

2.10.1.2. Em verificação no site do fabricante Broadcom (Symantec), quanto ao período de atuação/proteção do software, mesmo com o término da subscrição, tem-se informação que as *engines* de proteção continuam ativas, assim como as definições de antivírus continuam a ser carregadas, sem interrupções para o sistema de proteção, porém, acaba-se por utilizar tecnologia de proteção ultrapassada até que a solução seja substituída por nova tecnologia.

2.10.1.3. Quanto ao carregamento da database de informações sobre o tipo de vírus detectado, e reputação no painel gerencial EDR não serão mais carregados, assim como ocorrerá a perda do suporte no caso de eventuais falhas no software, erros e inconsistências. Ref. https://community.broadcom.com/symantecenterprise/communities/community-home/digestviewer/viewthread?MessageKey=3f03b24a-69e8-444d-9147-09ee8f2af44b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=digestviewer [Acesso em 07/01/2021].

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. Identificação das necessidades de negócio

3.1.1. A incidência de ataques contra órgãos e empresas públicas no âmbito da administração federal se tornou incisiva e recorrente nos últimos meses de 2020, onde os hackers exploraram diversas técnicas de invasão e disseminação, em busca de informações, através de motivações políticas ou partidárias, ou mesmo por disputas de regimes entre potências econômicas, como casos recentes aos ataques de hackers contra o STJ e TSE (Ataques de hackers STJ e TSE, acesso em 26/02/2021) ocorridos nos meses de novembro e dezembro de 2020, assim como o ataque ocorrido por grupo hacker da Rússia contra as agências norte americanas (Ataque hacker Russo às Agências dos EUA, acesso em 26/02/2021), através da contaminação de software de administração de redes de computadores, Solarwinds, ocorrido em dezembro de 2020.

3.1.2. As técnicas de ataques e exploração de vulnerabilidades evoluíram com o passar dos anos, antigas técnicas de ataques do tipo *Smurf attacks, Ping of Death (PoD),* que tratam de tentativas de exaustão da rede e dos sistemas operacionais não são mais utilizadas em detrimento de técnicas recompensatórias, como exemplo, malwares do tipo *ransomware*, e sequestro de dados para mineração de ativos monetários, as *crypto moedas* (conceito blockchain) utilizando ataques do tipo *cross-site scripting (XSS)*.

3.1.3. 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 instuição 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).

3.1.4. Com intuito de proteger os ativos da informação da VALEC, faz-se necessária a atualização tecnológica do software endpoint contra *malwares* baseado em comportamento e não mais em assinatura. O software baseado em comportamento (ATP) Next-Generation Antimalware 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 com proteção ativa, tendo proteção baseada em inteligência artifical - *machine learning* para proteções de malwares do tipo: Ransonware, Trojan, Spyware, Adware, Worms, rootkits, keyloggers, dentre outros.

3.2. **Identificação das necessidades tecnológicas**

3.2.1. A VALEC dispõe de software de segurança corporativo do tipo endpoint baseado em assinatura atualmente instalado e operacional em todas as estações de trabalho e servidores de sua rede corporativa, porém faz-se necessária atualização da engine de proteção para o tipo Next-Generation Antimalware que possui *engine* mais eficiente, sendo o agente mais leve (*lightweight*), não havendo a necessidade de varredura, oferecendo mecanismo de detecção, desempenho, e gerenciamento centralizado, tendo proteção ativa contra malwares baseado em inteligência artifical (*machine learning)* para proteções anti-malwares,aos principais malwares do tipo: Ransonware, Trojan, Spyware, Adware, Worms, rootkits, keyloggers, dentre outros.

3.2.2. Com a implementação e manutenção ativa do software de Endpoint Next-Generation , estabelece-se a proteção no parque tecnológico da VALEC para os principais tipos de ataques: proteção e exploração de ataques laterais através de disseminação de malwares nos segmentos de redes e pastas compartilhadas, proteção a arquivos acessados ou baixados na Internet, proteção contra malwares em dispositivos de mídias externas, ex. pendrivers, hd-externos, tokens, proteção a ataques a BIOS/UEFI, proteção a ataques de execução em memória.

3.2.3. Porém também há necessidade de rastreio das atividades do propenso malware, ou seja, de suas tentativas de execução e contaminação nas estações de trabalho, notebooks e servidores, sendo esta, uma das principais características de requisito técnico através da composição do agente, o módulo de proteção EDR, que permite por exemplo, a coleta das informações dos processos em execução da máquina e o motivo para a terminação dos processos, armazenando estas informações localmente e submetendo-as a console EDR.

3.2.4. Em suma, o módulo de análise forense de detecção e resposta EDR no agente endpoint permitirá a monitoração contínua dos eventos, captura e gravação em modo seguro das ações do malware, permitindo através da console EDR, a telemetria do malware, ou seja, visibilidade do tracejo das ações executadas pelo malware no endpoint ao qual foi detectado.

3.2.5. A partir da console EDR, têm-se o status das ameaças que foram detectadas para cada estação ou usuário, possibilitando aplicação de regras de remediação em conjunto com o agente do endpoint do tipo: bloqueio, quarentena, decisões de bloqueio, emissão de alerta da detecção, e isolamento do endpoint, aplicáveis a partir da classificação de reputação (severidade) baseadas em técnicas de ataque classificadas na framework MITRE ATT&CK®.

3.2.6. Os alertas de detecção e ações do malware, a depender da classificação do grau de severidade carregados na console EDR poderão ser repassados em tempo real através de API para ferramentas de correlacionamento de eventos de segurança do tipo SIEM, contendo informações do ataque, contribuindo para remediações e ações para a Gerência de Segurança da VALEC, formando um dos componentes para gestão de cibersegurança da estatal.

3.2.7. A vantagem do uso de solução ATP em relação a de assinatura, está diretamente relacionada a engenharia aplicada na análise comportamental do vírus, baseada em inteligência artificial, ou seja, o antivírus faz avaliações comportamentais dos processos executados pelos programas nativos dos sistemas operacionais e programas de terceiros que rodam nos SO's base, tipo Windows, MacOS, Linux, dentre outros. Na eventualidade de uma ação divergente a esperada, o antivírus aplica a proteção, pois na análise comportamental , o "programa executável" contaminado por um vírus, executa uma ação não esperada.

3.2.8. Já na solução em assinatura, existe uma vacina para o "programa executável" infectado pelo vírus, ou seja, no momento que este vírus infectou um programa ou arquivo, a vacina DAT, contém a instrução ou mapeamento da ação executada pelo vírus, aplicando a cura.

3.2.9. O problema ocorre, quando há possível "mutação" do vírus, onde é explorada outras "brechas" no computador ou software. Neste caso o antivírus será inoquo para esta nova ação, deixando o sistema vulnerável ao ataque.

3.3. **Quadro resumo do objeto de estudo deste ETP e proposta para contratação de softwares de segurança do tipo endpoint Next-Generation Anti-malware:**

1	Proteção dos ativos da informação da VALEC através de solução de segurança para endpoints usando tecnologia Next-Generation Antimalware com gerenciamento via console EDR na nuvem;
2	Proteger os ativos da informação da VALEC contra ameaças provenientes de sites, dispositivos externos e aplicativos que disseminam malware;
3	Criar camada de proteção contra malwares em infraestrutura on-premises para endpoints para proteger os ativos da informação a fim de garantir a integridade, disponibilidade e confidencialidade;
4	Ampliar o nível geral de segurança dos ativos da informação da VALEC, em conformidade com as mudanças realizadas na infraestrutura da rede local da VALEC;

4. CARACTERÍSTICAS DO AGENTE DE PROTEÇÃO CONTRA MALWARES

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

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

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

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

4.5. 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);

4.6. 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;

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

4.8. 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);

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

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

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

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

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

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

4.13. 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;

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

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

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

4.17. 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;

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

4.19. 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;

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

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

4.22. 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;

4.23. 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.

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

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

4.26. 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.

4.27. 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.

4.28. 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.

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

a) Alertar;

b) Bloquear.

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

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

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

a) ZIP;

b) RAR;

c) GZIP;

d) TAR;

e) JAR;

f) WAR.

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

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

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

4.36. 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;

4.37. 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;

4.38. 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;

4.39. 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.

5. MÓDULO DE ANÁLISE FORENSE E DETECÇÃO E RESPOSTAS (EDR)

5.1. 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;

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

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

5.4. 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;

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

5.6. 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;

5.7. 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;

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

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

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

5.11. 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;

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

5.13. Deve monitorar alterações em tarefas agendadas na máquina;

5.14. Deve monitorar tentativas de escalação de privilégios;

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

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

5.17. 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;

5.18. 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;

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

5.20. 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;

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

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

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

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

5.25. 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;

5.26. 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.

5.27. 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.

5.28. 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, Histórico do Browser, logs de execução de programas no Windows.

6. CARACTERÍSTICAS GERAIS DA CONSOLE DE GERENCIAMENTO PARA ENDPOINTS NEXT-GENERATION ANTIMALWARE DO TIPO EDR

6.1. 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;

6.2. 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;

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

6.4. 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.

6.5. 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;

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

6.7. 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.

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

6.9. 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;

6.10. 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;

6.11. 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;

6.12. 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;

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

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

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

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

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

6.18. 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;

6.19. 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;

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

6.21. 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;

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

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

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

6.25. 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.

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

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

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

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

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

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

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

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

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

6.35. 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.

6.36. 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;

6.37. 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;

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

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

6.40. 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;

6.41. 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;

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

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

6.44. 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;

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

6.46. 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;

6.47. Deverá possuir interface gráfica web, com suporte a um dos seguintes idioma:

a) Inglês;

b) Português do brasil.

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

6.49. 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;

6.50. 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;

6.51. 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;

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

6.53. 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;

6.54. Deve possibilitar instalação "silenciosa";

6.55. Deve permitir o bloqueio por nome de arquivo;

6.56. Deve permitir o rastreamento e bloqueio de infecções;

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

6.58. 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;

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

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

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

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

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

6.64. 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;

6.65. 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;

6.66. 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

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

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

6.69. 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;

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

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

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

6.73. 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;

6.74. Deve permitir a atualização automática dos agentes;

6.75. 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;

6.76. 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;

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

6.78. 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.

6.79. 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;

6.80. 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;

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

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

7. CONCLUSÃO ESPECIFICAÇÕES

7.1. As especificações descritas acima formam a solução de endpoint Next-Generation Anti-malware com respectiva proteção ativa.

7.2. A solução também inclui gerência EDR dispondo informações técnicas como exemplo: versão do agente, status de proteção, nome do endpoint, usuário, nome da máquina, eventos recentes e status de saúde.

8. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

8.1. A presente sessão contém o registro do quantitativo estimado de itens para a composição da solução a ser contratada, de forma detalhada, e justificada, inclusive quanto à forma de cálculo. Busca-se descrever também os métodos, metodologias e técnicas de estimativas que foram utilizados, nos termos do inciso I do art. 11 da IN SGD-ME n. 01/2019.

8.2. A principal análise é referente a quantidade de servidores que irão utilizar estações de trabalho e notebooks a serem protegidos pela solução de Next-Generation Antimalware atuando no âmbito da VALEC e de forma remota (teletrabalho).

8.3. Com o propósito de checar a quantidade de usuários ativos na VALEC foi realizada pesquisa na base de dados dos usuários da rede (serviço de diretório-autenticação).

8.4. Com o auxílio da ferramenta Power Bi, foram coletadas as informações necessárias para o quantitativo de usuários da rede conforme ilustra a imagem abaixo:

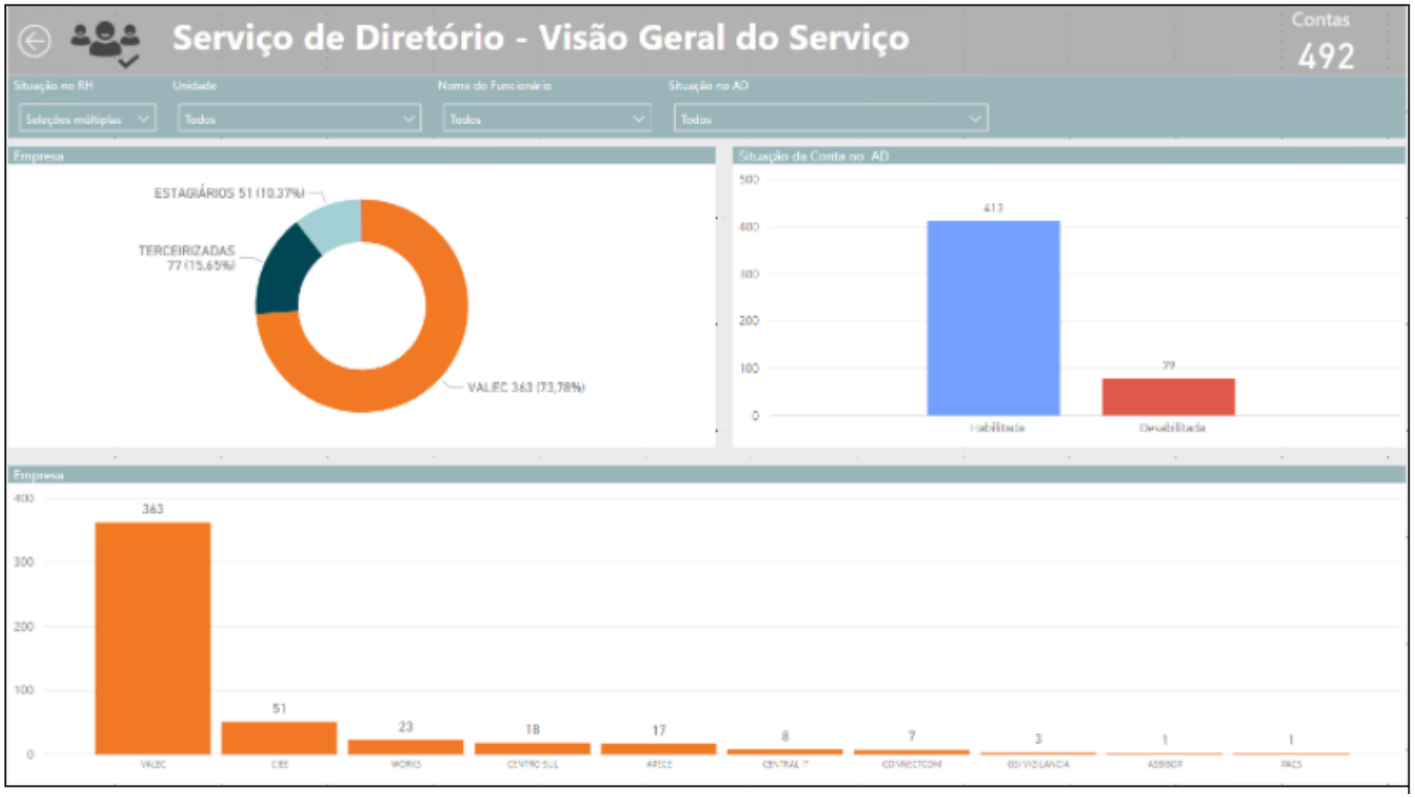


Fig. 01 - Painel de Usuários - Serviço de diretório - Visão Geral do Serviço (Extraído em 12/02/21) *Considerando o cenário atual com 79 contas desabilitadas.

8.5. No primeiro gráfico podemos observar que temos três tipos de usuários na empresa:

8.6. Usuários Valec: Compreendem servidores do quadro da VALEC, RFFSA, GEIPOT. Usuários que estão ativos, e não cedidos a outros órgãos. Estes usuários fazem uso dos computadores da empresa para execução diária de suas atividades laborais.

8.7. Usuários Estagiários: São estudantes de nível médio e superior. Cabe salientar que o contrato com o CIEE foi encerrado em dezembro último. Porém, na extração da informação do quantitativo, há época existiam 51 estagiários distribuídos nas 11 superintendências e 4 assessorias executando atividades administrativas de baixa complexidade e com prazo flexível para suas entregas, uma vez que são aprendizes. Há expectativa que seja celebrado novo contrato no primeiro semestre de 2021, atingindo o mesmo quantitativo.

8.8. Usuários Terceirizados: Compreende usuários de empresas com contratos ativos com a Valec, que prestam serviço em suas dependências, sejam elas obras ou dentro dos escritórios da Valec. Cabe esclarecer que a contratação desta solução não abrange a disponibilização de licenças ou computadores a empresas terceirizadas, uma vez que se tratam de recursos inerentes a prestação de serviço. Exceto em casos onde há previsão contratual de uso de recursos da contratante, como por exemplo os serviços de recepção, portaria ou suporte técnico, onde é desejável que a empresa use os mesmos recursos disponibilizados aos usuários com o propósito de compreender a perspectiva do usuário.

8.9. Nos gráficos subsequentes podemos observar como estes 3 grupos estão distribuídos na empresa. Cabe notar que neste painel o filtro utilizado foi da atual situação dos usuários e a empresa, excluindo usuários cedidos e terceirizados não habilitados ao uso do serviço. Por conta disto o total foi reduzido para 444 pessoas.

8.10. Da incorporação da EPL a Valec - Conforme matéria veiculada nos meios de comunicação conforme a publicação (3790025), onde o Ministério da Infraestrutura divulga o plano de incorporação da Empresa de Planejamento e Logística S.A. prevista para ocorrer no primeiro semestre de 2021. Cabe observar que foi celebrado o contrato de consultoria para estruturação do projeto, entre a Valec e a Empresa Falconi (51402.101308/2020-31), para estruturação técnica do projeto de incorporação. Até o momento ainda não foi possível estabelecer de maneira precisa o quantitativo final, logo foi considerado o quantitativo de funcionários efetivos daquela empresa, totalizando 121 pessoas, onde somando-se ao quadro de extração de dados da figura 01, têm-se o quantitativo final de 565 de usuários que serão cobertos pelas licenças a serem contratadas.

8.11. É necessário frisar que os servidores virtuais windows devem conter solução de segurança, sendo que atualmente há 48 servidores Windows, devendo ser considerado este quantitativo no total a ser demandado.

8.12. Baseado no estudo acima para atender a VALEC, estima-se a contratação dos seguintes itens, conforme tabela a seguir:

Item	Descrição	Qtd	Período
01	Fornecimento, instalação, configuração, manutenção e garantia de funcionamento de software de segurança para Endpoint Next-Generation (ATP) + 1 (uma) gerência EDR na nuvem (SaaS). Licença por endpoint corporativo.	565	36 meses
02	Fornecimento, instalação, configuração, manutenção e garantia de funcionamento de software de segurança para Endpoint Next-Generation (ATP) para servidores windows	48	36 meses

9. ANÁLISE DE SOLUÇÕES

9.1. O tipo de proteção de endpoint atualmente implementado no ambiente corporativo da VALEC é baseado em assinatura, sendo este modelo considerado ultrapassado, em face de novas tecnologias, como a proteção baseada em comportamento, Next-Generation Antimalware - (ATP) *Advanced Threat Protection.*

9.2. Em face desta nova tendência que o mercado corporativo está seguindo, justificado pela atualização tecnológica na proteção de malwares em decorrência do aprimoramento de ataques, tendo como referência, a consulta de estudo realizado em outubro de 2020 por entidade Austríaca situada em Innsbruck (https://www.av-comparatives.org/imprint/), chamada "AV-Comparatives GmbH", [Acesso em 06/01/2021] que faz a comparação de soluções de antivirus, é importante considerar, a aquisição de software para endpoints do tipo Next-Generation Antimalware - (ATP) *Advanced Threat Protection* baseado em comportamento,

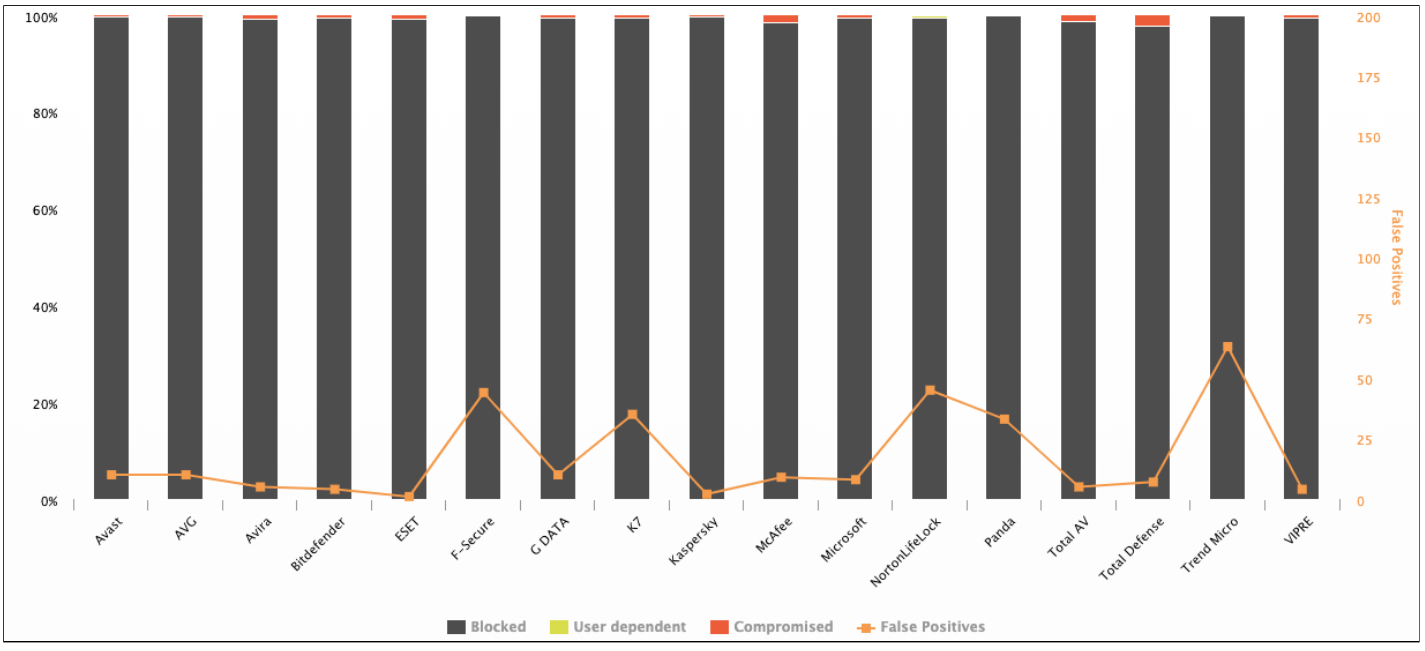


Fig. 02 - Comparativo de Soluções AV-Comparatives GmbH. Fonte: https://www.av-comparatives.org/imprint/

9.3. Órgãos, como o INEA/RJ Instituto Estadual do Ambiente, planejam a contratação de software utilizando a solução Next-Generation. Registra-se que na data de 06 de janeiro de 2021, a equipe da GSINF/SUPTI participou como convidada de uma POC da solução Next-Generation do fabricante CrowdStrike, apresentada pela empresa NIVA TI.

10. IDENTIFICAÇÃO DAS SOLUÇÕES

1	Solução de segurança para endpoints usando tecnologia de detecção Next-Generation Anti-malware baseada em comportamento (ATP) + gerência EDR na nuvem (SaaS)
2	Solução de segurança para endpoints usando tecnologia de detecção Next-Generation Anti-malware baseada em comportamento (ATP) + gerência EDR on-premises (local)

10.1. Análise Comparativa de Soluções

10.1.1. Esta Gerência de Segurança da Informação GSINF/SUPTI/DIRAF, fez levantamento das principais soluções aplicáveis a proteção de endpoint e softwares para proteção de ativos da informação, sendo a tendência de uso pelas empresas, a escolha por softwares do tipo Next-Generation Antimalware para proteção das estações e servidores alocados na infraestrutura on-premises (local) baseado nos seguintes fundamentos:

a) estudos das normas brasileiras e internacionais de segurança da informação, ISO 27001/27002/27005/17799;

b) da IN 01 de abril de 2019 do SGD;

c) das leis de proteção de dados LGPD e GDPR;

d) da tendência de uso das tecnologias de proteção;

e) da aplicabilidade da solução em órgãos do governo federal e estadual através de ETP's e contratações nos portais, SEI, ComprasNet, e Pesquisa de Preços;

f) da consulta de software de disponibilidade de software em sítios do portal de Software Público Brasileiro;

g) dos testes de detecção de malwares para os softwares de endpoint, realizados por entidades internacionais como Gartner, e AV-Comparatives GmbH;

h) do contato realizado com fornecedores solicitando apresentação das soluções comercializadas;

10.2. Da solução 1 - Solução de segurança para endpoints usando tecnologia de detecção Next-Generation Anti-malware baseada em comportamento (ATP) + gerência EDR na nuvem (SaaS)

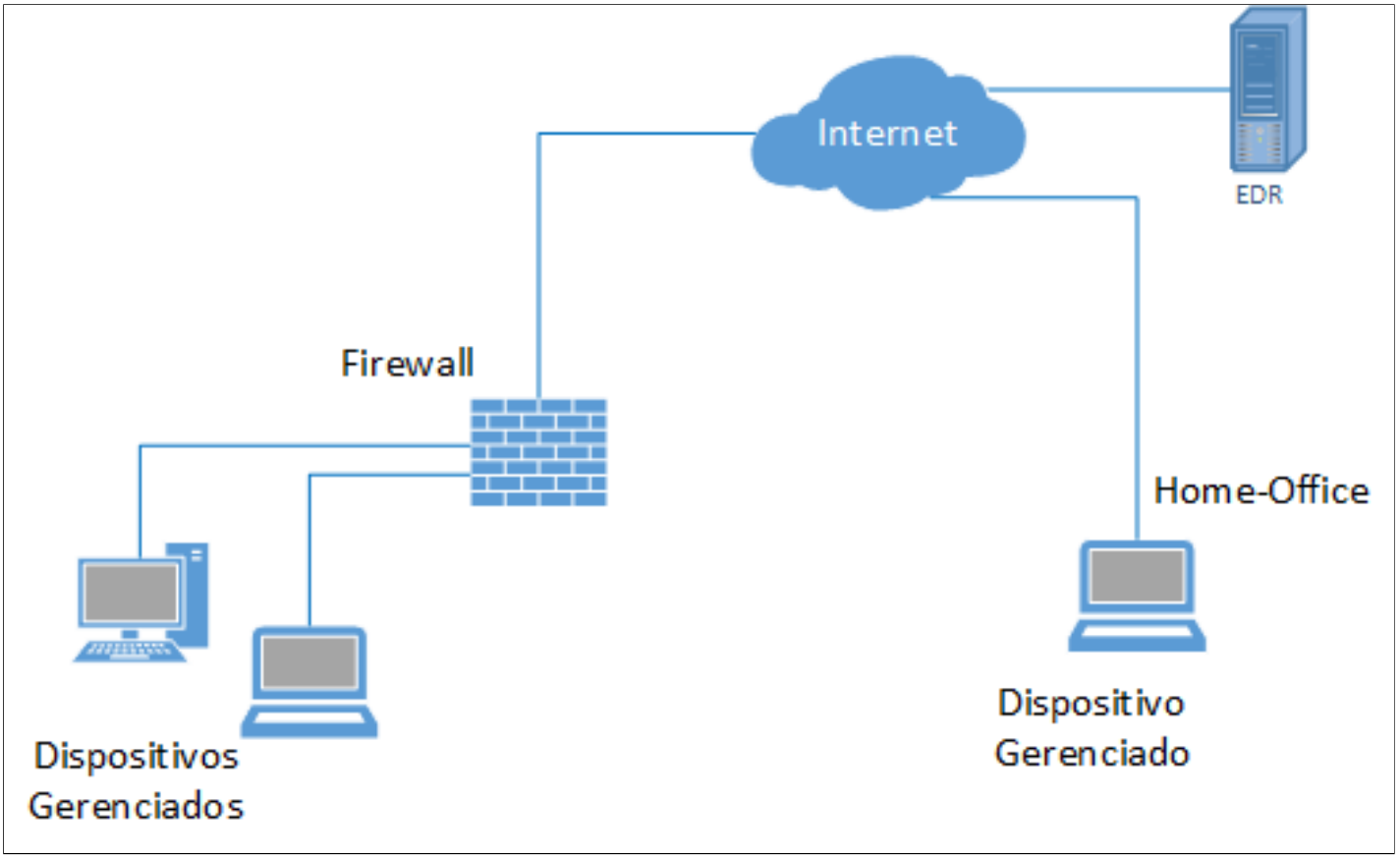


Fig. 03 - Topologia tipo 1 para solução Next-Generation Anti-Malware + gerência EDR na nuvem (SaaS)

10.2.1. Nesta solução, os endpoints corporativos possuem agentes e são gerenciados pela ferramenta de gerência EDR localizada na nuvem (SaaS). Mesmo os endpoints localizados fora da dependência da VALEC, estes continuam sendo gerenciados pela gerência

EDR na nuvem através de conexão segura (SSL) sujeitos a mesma política, desde que estejam com o agente do endpoint Next-Generation Anti-malware instalado.

10.3. **Da solução 2 - Solução de segurança para endpoints usando tecnologia de detecção Next-Generation Anti-malware baseada em comportamento (ATP) + gerência EDR on-premises (local)**

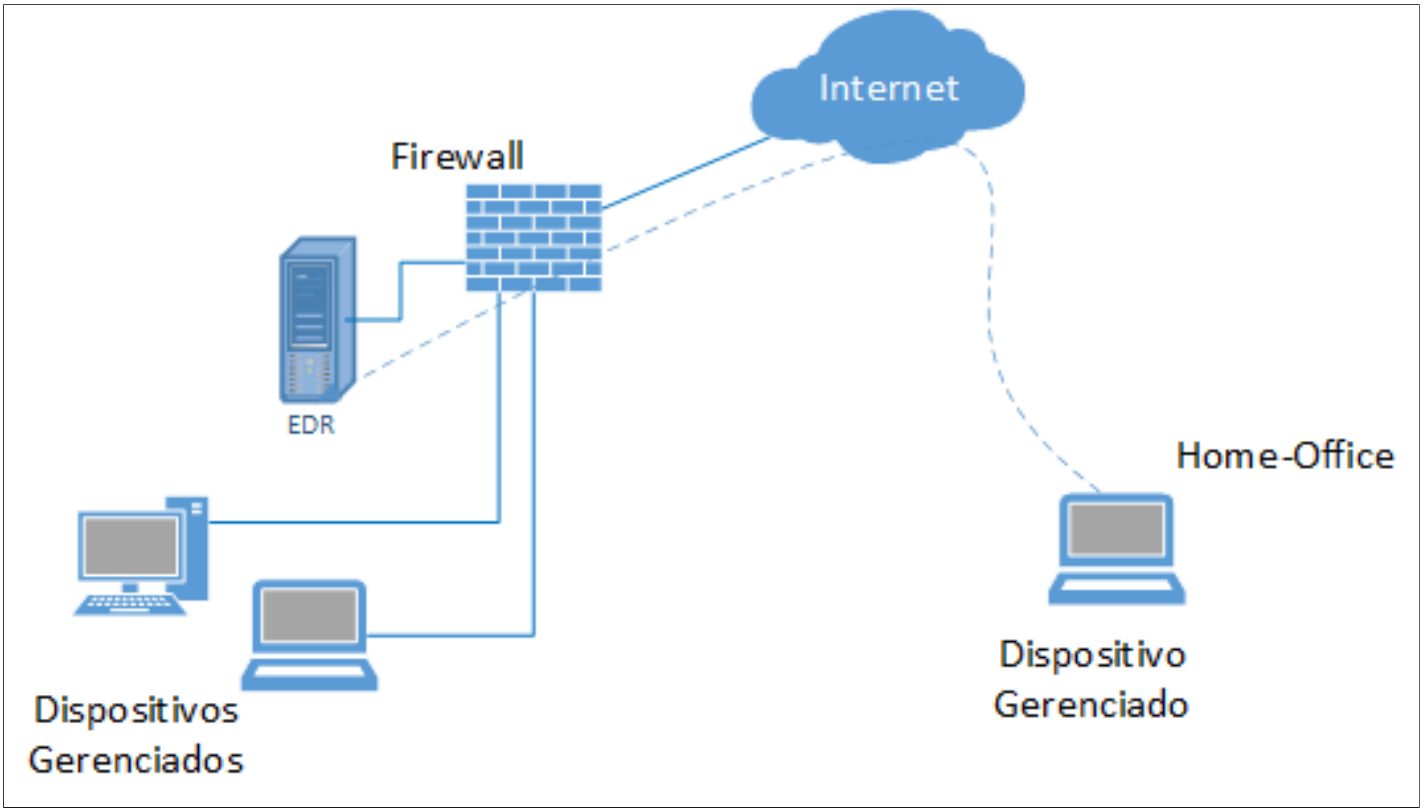


Fig. 03 - Topologia tipo 2 para solução Next-Generation Anti-Malware + gerência EDR on-premises (local)

10.3.1. Nesta solução 2, os endpoints corporativos possuem agentes e são gerenciados pela ferramenta de gerência EDR, de forma parecida com a solução 1, com a diferença da gerência EDR ser uma máquina virtual (VM) posicionada no ambiente local (on-premises). Mesmo os endpoints localizados fora da dependência da VALEC, estes continuam sendo gerenciados pela gerência EDR no ambiente local (on-premises) de forma remota através de conexão segura (SSL) sujeitos a mesma política, desde que estejam com o agente do endpoint Next-Generation Anti-malware instalado.

10.4. Abaixo segue comparativo por amostragem dos principais fabricantes do mercado, independente da localização da gerência EDR, atualmente ofertadas ou mantidas por eles:

Fabricante	Produtos	Tipo de proteção (ATP Next-Gen/Assinatura)
Crowdstrike	Falcon Pro/Enterprise/Premium	ATP Next-Gen
TrendMicro	Apex One	ATP Next-Gen
Microsoft	Windows Defender for Endpoint	ATP Next-Gen
Sophos	Intercept X Endpoint	ATP Next-Gen

Quadro 01 - Comparativo tipo de soluções

1- https://www.trendmicro.com/pt_br/business/products/user-protection/sps/endpoint.html [Acesso em 11/02/2021]

2- https://www.crowdstrike.com/endpoint-security-products/falcon-endpoint-protection-pro/ [Acesso em 11/02/2021]

3- https://docs.microsoft.com/en-us/windows/security/threat-protection/ [Acesso em 11/02/2021]

4- https://www.sophos.com/en-us/products/endpoint-antivirus/edr.aspx [Acesso em 11/02/2021]

10.5. Observa-se que os fabricantes atualmente ofertam seus produtos de endpoint utilizando tecnologia baseada em comportamento (ATP) frente a tecnologias ultrapassadas, baseadas em assinatura, fato real, visto que institutos de pesquisa como a AV-TEST GmbH, são especialistas em testar e evidenciar o que os softwares dispõem a fazer para proteção a ataques de malware, baseados nas tendências e técnicas de ataque atualmente exploradas pelos hackers.

10.6. Como os padrões de ataques variam constantemente, ou seja, numa simples alteração de código do malware a partir da criação de uma segunda versão ou analogamente, uma "mutação" do código genético do vírus, o atacante pode levar vantagem frente a solução de endpoint baseada em assinatura, visto que, a vacina específica para o malware, mapeada na primeira variação do "vírus", não está mapeada para a segunda, ou seja, não tem vacina para a "mutação", desta forma, a solução baseada em assinatura não traz a proteção efetiva contra novas variações e formas de ataques, sendo indicada solução com tecnologia Next-Generation Antivirus baseada em análise comportamental (*machine learning).*

10.7. De setembro a novembro de 2020, foram realizados pela AV-Comparatives testes de proteção a ataques cibernéticos para o mundo real - "*Enhanced Real-World Test 2020 – Enterprise*" para os principais endpoints de mercado*. Fonte: https://www.av-comparatives.org/tests/enhanced-real-world-test-2020-enterprise/ - [Acesso em 06/01/2021]. Segue detalhes dos testes, a seguir.

*Alguns fabricantes de Endpoint Next-Generation recusaram a participação dos testes de carácter colaborativo realizado pela AV-Comparatives, como informado pela Av-comparatives no item 9.10.2.

10.8. **Dos testes realizados [**AV-Comparatives]

10.8.1. *O escopo do teste consistiu em testar os produtos contra métodos de ataques específicos, não considerando a proteção total do software, ou como protege bem o sistema contra um malware "baixado" da Internet ou introduzido via dispositivos USB. O teste foca em como os produtos de segurança protegem contra técnicas de ataques específicos usados em ameaças de persistência avançada (APT - Advanced Persistent Threats).*

10.9. **Procedimento dos testes**

10.9.1. *"Scripts de macro como VBS, JS, MS Office podem executar e instalar um backdoor sem arquivo "file-less" no sistema da vítima e criar um canal de controle (C2 - malware command e control também conhecido como C&C - Grifo GSINF) para o atacante que geralmente está em uma localização física diferente, ou mesmo em um país diferente. Além desses cenários bem conhecidos, é possível fazer a entrega de malware usando exploits, chamadas remotas (remote call), como PSexec, wmic, agendador de tarefas (task manager), entradas de registro, Hardware Arduino (USB RubberDucky) e chamadas WMI. Isso pode ser feito com ferramentas integradas do Windows como PowerShell. Esses métodos carregam o malware diretamente da Internet para o alvo memória do sistema, e continua a expandir ainda mais para a rede local com ferramentas nativas do sistema operacional. Eles podem até se tornar persistentes nas máquinas dessa maneira. O teste deste ano não faz uso de malware executável portátil (PE). No entanto, como a natureza das ameaças persistentes avançadas continuam a evoluir, podemos introduzir um ou dois exemplos destes no futuro, se apropriado.*

10.10. **Ataques sem arquivos (Fileless attacks)**

10.10.1. *No campo do malware, existem muitas categorias de classificação (possivelmente sobrepostas), e entre outras coisas, uma distinção pode ser feita entre malware baseado em arquivo (file-based) e malware sem arquivo (fileless). Desde 2017, um aumento significativo em ameaças sem arquivo (fileless) foi registrado. Uma razão para isso é o fato de que esses ataques tem provado serem muito bem-sucedidos do ponto de vista dos atacantes. Um fator em sua eficácia é o fato de que ameaças sem arquivo operam apenas na memória do sistema comprometido, tornando-o mais difícil para as soluções de segurança reconhecê-los."*

10.11. **Vetores e alvos de ataques (Attack vectors and targets)**

10.11.1. *Em testes de penetração, vemos que certos vetores de ataque podem ainda não estar bem cobertos pela segurança de programas, e muitos produtos AV populares ainda fornecem proteção insuficiente. Alguns produtos de segurança empresarial estão agora fazendo melhorias nesta área e fornecendo melhor proteção em alguns cenários. Conforme mencionado acima, acreditamos que os produtos de consumo também precisam melhorar suas proteções contra tais ataques maliciosos; usuários não empresariais podem ser, e são, atacados na mesmo caminho. Qualquer pessoa pode virar alvo, por uma variedade de razões, incluindo "doxing" (publicação confidencial de informações pessoais) como um ato de vingança. Atacar os computadores domésticos de empresários também é uma rota óbvia para acessar os dados da empresa.*

10.12. **Métodos de ataques (Attack methods)**

10.12.1. *No teste de proteção avançada contra ameaças (ATP), também incluímos várias pilhas de linha de comando diferentes, CMD/PS, que podem baixar malware da rede diretamente para a RAM ou chamadas codificadas em base64. Esses métodos evitam completamente o acesso ao disco, que (geralmente) é bem protegido por produtos de segurança. Às vezes, usamos medidas de ocultação simples ou mudamos o método do stagger call também. Depois que o malware carrega seu segundo estágio, uma conexão http/https com o invasor será estabelecido. Este mecanismo de dentro para fora tem a vantagem de estabelecer um canal C2 para o invasor que está além das medidas de proteção da maioria dos produtos de NAT e firewall. Uma vez que o túnel C2 foi estabelecido, o invasor pode usar todos os mecanismos de controle conhecidos de produtos C2 comuns (Meterpreter, PowerShell Empire, etc.). Estes incluem, por exemplo, arquivo uploads / downloads, capturas de tela, keylogging, shell do Windows (GUI) e webcam snapshots. Todos as ferramentas utilizadas estão disponíveis gratuitamente. Seu código-fonte é aberto e criado para fins de pesquisa. Contudo, os bandidos costumam abusar dessas ferramentas para fins criminosos.*

10.13. **Falso Positivo (False Alarm Test)**

10.13.1. *Um produto de segurança que bloqueia 100% dos ataques maliciosos, mas também pode bloquear ações legítimas (non-malicious), sendo extremamente disruptivos. Consequentemente, realizamos um teste de falsos positivos como parte do Teste de proteção avançada (ATP) contra ameaças, para verificar se os produtos testados são capazes de distinguir as ações de malwares maliciosos ou não. Caso contrário, um produto de segurança poderia bloquear facilmente 100% de ataques maliciosos que, por exemplo, use anexos de e-mail, scripts e macros, simplesmente bloqueando tais funções. Para muitos usuários, isso pode impossibilitar a*

realização de suas tarefas diárias normais. Consequentemente, as pontuações de falso-positivo são levadas em consideração na pontuação do teste do produto.

10.14. **Produtos testados**

10.14.1. *Os seguintes fabricantes participaram do testes de Proteção Avançada Contra Ameaças (ATP): Este são fabricantes onde seus produtos são confidentes o suficiente para as capacidades de proteção contra ameaças que farão parte deste teste.*

Vendor	Product	Version
Avast	Business Antivirus Plus	20.7
Bitdefender	GravityZone Elite Security	6.6
CrowdStrike	Falcon Pro	5.41 - 6.12
ESET	Endpoint Protection Advanced Cloud[3]	7.2
Fortinet	FortiClient with FortiSandbox and FortiEDR	6.4
Kaspersky	Endpoint Security for Business Select	11.4
SparkCognition	DeepArmor Endpoint Protection Platform	3.4
Vipre	Endpoint Security Cloud	12.0

Fig. 05 - Produtos dos fabricantes e respectivas versões de software (ATP) sujeitas ao teste

10.14.2. Como informado no item 9.3.5 "*Alguns endpoint recusaram a participação dos testes de carácter colaborativo realizado pela AV-Comparatives, assim como não participaram com seus respectivos produtos EDR, ou desabilitaram os componentes EDR de seus produtos.

> *"Most AV vendors did not participate with their respective EDR products, or disabled the EDR components of their participating products (see settings below). This may be explained by the following. The Enterprise ATP Test is an optional add-on to the Enterprise Main Test Series. We use the same product and configuration for all the tests within a series, and some EDR functions can have a negative impact on performance and false alarms."*

10.14.3. **Nota (GSINF)**: Apesar de fabricantes como Microsoft, Trend Micro, Sophos não terem participado dos testes, o produtos destes fabricantes estão classificados como "Leader" no quadrante mágico do Gartner, atendendo a todos os requisitos de proteção da solução, de acordo com o item 4. Vide quadrante abaixo:

Fig 06 - Quadrante mágico Gartner - Endpont Protection Platforms
Fonte: https://www.microsoft.com/security/blog/2019/08/23/gartner-names-microsoft-a-leader-in-2019-endpoint-protection-platforms-magic-quadrant/

10.15. **Configurações**

10.15.1. Em ambientes corporativo e com produtos corporativos em geral, é usual que o administrador configure os produtos de acordo com os manual do fabricante, desta forma, todos os fabricantes foram convidados a configurarem seus respectivos produtos. Abaixo, foram listados as configurações aplicadas pelos fabricantes, editando as configurações para otimização de proteção, em comparação as configurações padrão.

10.15.2. Nota: Observe que os resultados alcançados são válidos apenas para os produtos testados com suas respectivas configurações. Com outras configurações (ou produtos) a pontuação pode ser pior ou melhor.

Avast, Vipre: default settings.
Bitdefender: "Sandbox Analyzer" and "Scan SSL" enabled; "HyperDetect", "Device Sensor" and "EDR Sensor" disabled.
CrowdStrike: everything enabled and set to maximum, i.e. "Extra Aggressive". "Unknown Detection-Related Executables" and "Unknown Executables" disabled.
ESET: All "Real-Time & Machine Learning Protection" settings set to "Aggressive".
Fortinet: All "AntiVirus Protection" settings enabled and set to "Block". Additionally, "Anti-Exploit", "Cloud Based Malware Detection", "Advanced Heuristic", "FortiGuard Analytics", FortiSandbox's "Sandbox Detection", "Web Filter", "Application Firewall", "Detect and Block Exploits & Botnets" and "FortiEDR" were all enabled; "Exclude Files from Trusted Sources" for "Sandbox Detection" enabled.
Kaspersky: "Adaptive Anomaly Control" disabled.
SparkCognition: all "Policy Settings" and all "Attack Vectors" settings enabled and set to "Aggressive".

Please note that the results reached are valid only for the products tested with their respective settings. With other settings (or products) the scores could be worse or better.

Fig. 07 - Configurações de proteção ATP aplicadas pelo respectivo fabricante do software Next-Gen ATP.

10.16. **Caso de testes empregados**

10.17. Usamos cinco diferentes fases de acesso inicial, distribuídas entre os 15 casos de teste (por exemplo, 3 casos de testes vieram por e-mail / anexo de spear-phishing).

a) Relação de confiança: "Os adversários podem violar ou de outra forma alavancar organizações que têm acesso às vítimas pretendidas. O acesso por meio de relacionamento confiável com terceiros explora uma conexão que pode não ser protegida ou recebe menos escrutínio do que os mecanismos padrão de obter acesso a uma rede."

b) Contas válidas: "Os adversários podem roubar as credenciais de um usuário específico ou conta de serviço usando Técnicas de acesso à credencial ou captura de credenciais no início do processo de reconhecimento por meio Engenharia social [...]."

c) Replicação por meio de mídia removível: "Os adversários podem mover-se para os sistemas [...] copiando malware para mídia removível [...] e renomeá-lo para parecer um arquivo legítimo para enganar os usuários executá-lo em um sistema separado. [...] "

d) Phishing: anexo de spearphishing: "O anexo de spearphishing é [...] emprega o uso de malware anexado a um e-mail. [...] "

e) Phishing: Spearphishing Link: "Spearphishing com um link [...] emprega o uso de links para baixar malware contido em e-mail [...]. "

10.18. Os 15 cenários de testes usados neste teste são descritos resumidamente a seguir:

1. Essa ameaça é introduzida por meio de relacionamento confiável. MSHTA lança um aplicativo HTML, que executa uma carga útil do Empire PowerShell em estágio.
2. Essa ameaça é introduzida por meio de relacionamento confiável. Um script PowerShell contendo um bypass AMSI e um stager PowerShell Empire foi executado.
3. Essa ameaça é introduzida por meio de relacionamento confiável. O Windows Scripting Host foi usado para fazer o download uma carga útil do PowerShell por meio de um Empire PowerShell Stager integrado, combinado com um bypass AMSI.
4. Essa ameaça é introduzida por meio de contas válidas. O confiável utilitário do Windows Microsoft Build O motor foi usado como proxy para a execução de uma carga de macro Empire, que abre um comando e canal de controle.
5. Essa ameaça é introduzida por meio de contas válidas. Um VBScript que gera um processo PowerShell e executa uma carga útil do Império foi usada.
6. Essa ameaça é introduzida por meio de contas válidas. Um arquivo em lote foi usado para executar um ofuscado Stager do PowerShell, baixe uma carga útil PoshC2 ofuscada.
7. Esta ameaça é introduzida por meio de mídia removível (USB). Um JavaScript executa um ofuscado Stager do PowerShell, que baixa e executa uma carga útil PoshC2 PowerShell.
8. Esta ameaça é introduzida por meio de mídia removível (USB). MSHTA.exe executa um stager do PowerShell que inicia uma carga útil do PowerShell encadeada PoshC2 codificada em base64.
9. Esta ameaça é introduzida por meio de mídia removível (USB). Uma macro maliciosa do Microsoft Office é executada uma carga útil PoshC2 PowerShell. Teste de proteção avançada contra ameaças 2020 (Enterprise) www.av-comparatives.org
10. Essa ameaça é introduzida por meio do Anexo de Spearphishing. O VBScript baixa e executa um XSL Carga útil PoshC2.
11. Essa ameaça é introduzida por meio do Anexo de Spearphishing. Um aplicativo HTML é baixado e executa uma carga útil do PowerShell ofuscada. Este caso de teste foi criado com Metasploit Meterpreter.
12. Esta ameaça é introduzida por meio do anexo de Spearphishing. O VBScript baixa e executa um XSL carga útil. Este caso de teste foi criado com Metasploit Meterpreter.
13. Essa ameaça é introduzida por meio do link Spearphishing. MSHTA.exe baixa e executa um carga útil XSL ofuscada. Este caso de teste foi criado com Metasploit Meterpreter.
14. Essa ameaça é introduzida por meio do link Spearphishing. Um JavaScript baixa e executa um carga útil ofuscada do PowerShell. Este caso de teste foi criado com Metasploit Meterpreter.
15. Essa ameaça é introduzida por meio do link Spearphishing. MSHTA.exe baixa e executa um PowerShell stager, que baixa e executa uma carga útil PowerShell testada PowerShell Empire criptografada combinado com um desvio AMSI.

10.19. ***Resultado dos Testes***

10.19.1. *Abaixo segue resultados dos 15 ataques usados neste teste de proteção avançada contra ameaças (ATP)*

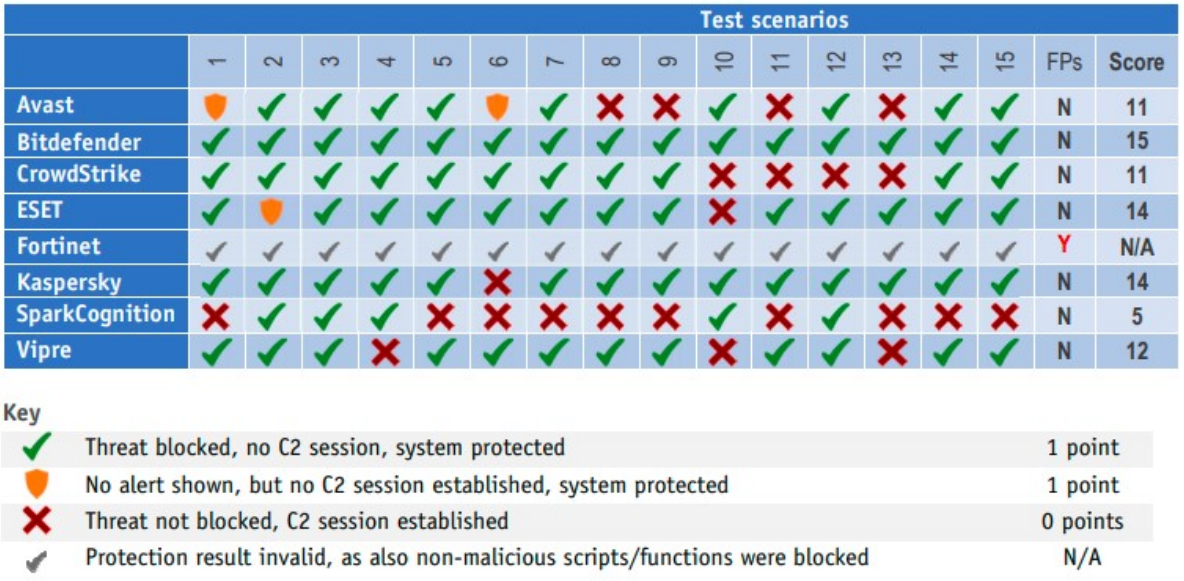


Fig. 08 - Resultado dos 15 ataques usados neste cenário de testes

10.19.2. *... Todos os fabricantes continuam aprimorando seus produtos, então é esperado que alguns de ataques não identificados usados nos testes sejam agora cobertos."* pela Av-comparatives. Fonte: https://www.av-comparatives.org/wp-content/uploads/2020/12/avc_atp_2020_12_ent.pdf [**Acesso em 11/02/2021**]

10.19.3. Abaixo segue quadro comparativo conforme inciso II do art. 11, sendo feita verificação para composição da análise comparativa:

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X

Quadro 02 - quadro comparativo de soluções conforme inciso II do art. 11

11. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

11.1. Soluções baseadas em assinatura são consideradas ultrapassadas e sujeitas a exploração de vulnerabilidades elevadas, sendo desta forma inviáveis na proteção ativa aos endpoints, justificado pelo avanço tecnológico das ameaças (malwares), de acordo com os testes realizados no item 10.8 a 10.17.

11.2. A solução 2, é considerada inviável para VALEC, pois os fabricantes não disponibilizam a gerência EDR posicionada na infraestrutura local do cliente (on-premises), somente se por especificidade da regra de negócios do cliente, como exemplo, bancos e agências de inteligência, que não podem ter informações de dispositivos endpoints, ou outras que compõem a solução, armazenada na gerência EDR posicionada na nuvem.

12. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

12.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 6.1 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

13. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

13.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 6.2 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

14. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

14.1. A VALEC dispõe de software de segurança corporativo do tipo endpoint baseado em assinatura atualmente instalado e operacional em todas as estações de trabalho e servidores de sua rede corporativa, porém faz-se necessária atualização da engine de proteção para o tipo Next-Generation Antimalware sendo mais eficiente, através da utilização de agente mais leve do tipo *lightweight*, oferecendo mecanismo de detecção, desempenho, e gerenciamento centralizado, tendo proteção ativa contra malwares utilizando tecnologia de detecção baseado em inteligência artifical (*machine learning).*

14.2. Neste interim, em atendimento as boas práticas de segurança da informação, considerando a IN 01 de 04 de abril de 2019, do SISP, é vedada a contratação para criação ou ampliação de salas-cofre e salas seguras, devendo as entidades e órgãos que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação. Desta forma, é instruído as entidades e órgãos o incentivo por contratar soluções de computação em nuvem.

14.3. Ainda, da PSI - Política de Segurança da Informação da VALEC - esta estabelece através do item 2.3, do Objeto "*Prevenir possíveis causas de incidentes, com possível responsabilização da instuição 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 necessária proteção aos ativos da informação da VALEC através de software de segurança para Endpoint Next-Gen Anti-malware, estabelecendo uma camada de proteção ativa para estes, respectivamente através de mecanismo de proteção baseado em comportamento usando inteligência artificial (machine learning).

14.4. Observado tais parâmetros, optou-se pela gerência EDR na nuvem (SaaS), descrita na solução viável 1, sendo considerada mais vantajosa, devido ao valor total e disponibilidade proporcionada pelo fornecedor que deve obedecer SLA de 99,9%, de acordo com o item 6.6.

14.5. Ao se realizar o estudo demonstrado no item 10 deste ETP, observou-se que a solução Microsoft Defender ATP (Advanced Threat Protection) devido sua ampla integração com o ecossistema de soluções da microsoft que já utilizamos, como servidores, banco de dados, sistema operacional para estações de trabalho, servidor de arquivos, solução de cliente de e-mail, solução de videoconferência e outras soluções de outros fabricantes que já utilizamos, permite gestão unificada com poucos profissionais e respostas mais rápidas a ameaças aos dados e serviços da Valec, considerando os recentes acontecimentos decorrentes da pandemia de COVID-19 onde em curto espaço de tempo os colaboradores da empresa, passaram a exercer suas atividades remotamente e computadores pessoais, aumentando o nível de exposição a ameaças digitais se fazendo urgente ação de gestão contratar solução que atenda a nova gama de requisitos e necessidades enfrentadas pela empresa. A solução em questão como parte integrante de contratação maior a ser adquirida, conforme demonstrado no documento SEI 3715695 promove diversos fatores tecnicamente vantajosos tendo em vista que os serviços de proteção a ameaças digitais se tornaram serviço de caráter continuado, devido a sua recorrente necessidade de contratação nos últimos anos, observa-se também que as ameaças digitais mudam diariamente e simplesmente atualizar definições de segurança já não são mais suficientes em face a evolução das ameaças.

14.6. Nota-se também que em comparação a soluções de outros fabricantes a partir do mapa comparativo constante na Análise Comparativa de Custos, item 12 deste ETP, em alguns casos, podem até apresentar um custo financeiro ligeiramente menor, entretanto há que se observar a vantajosidade técnica oferecida pela solução Microsoft Defender ATP (Advanced Threat Protection), onde através **da integração com a solução de segurança CASB - Microsoft Cloud App Security (MCAS)** (SEI 3715695), proporciona gestão mais efetiva, uma vez que trata logs, ações e detecções de comportamento de maneira centralizada, reduzindo riscos quanto a ácuracia e tempo de resposta na análise de uma ameaça ou aplicação não-sancionada. Dentre estas importantes integrações, 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 Antivírus dentro do SLA de proteção de rede.

VIII - Integração entre o serviço de identidade do Microsoft Azure AD (Azure AD Identity Protection);

IX - Dentre outras. Fonte: https://docs.microsoft.com/en-us/cloud-app-security/mde-integration#investigate-devices-in-cloud-app-security [Acesso em 23/02/2021]

15. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

15.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 6.3 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

16. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

16.1. Não se aplica tendo em vista tratar-se de um produto único.

17. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

17.1. Não se aplica.

18. PROVIDÊNCIAS A SEREM ADOTADAS ANTES DA CONTRATAÇÃO

18.1. Como o ambiente atual da Valec já possui o licenciamento da referida ferramenta, não há providências prévias a serem adotadas.

19. ANÁLISE DE CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

19.1. Conforme Termo de Referência SEI 3734548 , itens 5.6 e 8.

20. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS DE TRATAMENTO

20.1. Conforme Termo de Referência SEI 3734548 , itens 5.6 e 8.

21. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

21.1. A solução de segurança para endpoint Next-Generation protegerá 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.

21.2. Nesse sentido, o planejamento em tela almeja os seguintes resultados:

- Economia no valor da aquisição;
- Eficiência com a redução do custo administrativo em função da redução da fragmentação de processos licitatórios;
- Efetividade com a padronização dos produtos e com a promoção de segurança mais profunda das informações;
- Eficácia com o atendimento das necessidades tecnológicas e de negócio da Valec.

21.3. Com intuito de proteger as atividades de negócio 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, em tempo real, tendo proteção baseada em inteligência artifical - *machine learning* para proteções de malwares do tipo: Ransonware, Trojan, Spyware, Adware, Worms, rootkits, keyloggers, dentre outros.

21.4. Das vantagens da escolha e utilização da solução 1 para Endpoin Next-Generation Anti-Malware com gerência EDR na nuvem (SaaS), destacam-se:

I - Proteção ativa para Endpoint contra ações de malwares utilizando tecnologia de proteção a ameaças avançadas (ATP) - Endpoint Next-Generation (NGAV) baseada em comportamento (*machine learning).*

II - Propiciar proteção aos ativos da informação da VALEC contra ameaças anti-malware;

III - Propiciar gerenciamento dos Endpoints Next-Gen Anti-malware através da console EDR posicionada na nuvem (SaaS) com SLA de funcionamento do fornecedor/fabricante de 99,9%;

IV - Solução a ser adquirida e implementada estará em consonância com a PSI da VALEC e IN 01 2019 da SGD.

V - Proteção a infraestrutura de segurança dos dados armazenados na instituição e carregados na nuvem provendo confidencialidade, integridade e disponiblidade das informações trafegadas e armazenadas nas estações de trabalho e servidores nos mais diversos sistemas corporativos da VALEC.

21.5. Considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente **VIÁVEL.**

22. APROVAÇÃO E ASSINATURA

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

22.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
_____ **CLÁUDIO AMORIM DE SOUSA**	_____ **ROBÉRIO XIMENES DE SABÓIA** **Matrícula/SIAPE: 1990222**

Matrícula/SIAPE: 3218987	

AUTORIDADE MÁXIMA DA ÁREA DE TIC **(OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)**
_____ **JORGE LUIS DA SILVA LUSTOSA** **Matrícula/SIAPE: 1105206**

Documento assinado eletronicamente por **Jorge Luis da Silva Lustosa**, **Superintendente**, em 01/03/2021, às 19:03, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Cláudio Amorim de Sousa**, **Gerente**, em 01/03/2021, às 19:04, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Sabóia**, **Integrante Requisitante**, em 01/03/2021, às 20:24, conforme horário oficial de Brasília, com fundamento no art. 3°, 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 **3715636** e o código CRC **DC04151B**.

Referência: Processo nº 51402.100731/2020-14 SEI nº 3715636

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

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

Estudo Técnico Preliminar da Contratação/GEINF-VALEC/SUPTI-VALEC/DIRAF-VALEC-VALEC

Brasília, 02 de fevereiro de 2021.

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
26/01/2021	1.0	Elaboração da primeira versão do documento	Luciane Inácia Lopes
05/02/2021	2.0	Revisão da primeira versão do documento	José Augusto Meira Rocha
27/02/2021	2.1	Revisão prévia de envio ao setor de licitações	Jorge Luis da Silva Lustosa

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Referência: IN SGD/ME nº 1/2019.

1. INTRODUÇÃO

1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda SEI 3781122, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. Durante o Estudo Técnico Preliminar, diversos aspectos devem ser levantados para que os gestores certifiquem-se de que existe uma necessidade de negócio claramente definida, há condições de atendê-la, os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente.

1.3. O objeto do estudo é a contratação de **Sistema gerenciador de banco de dados** que atenda de forma ampla as demandas da Valec Engenharia, Construções e Ferrovias S.A.

2. MOTIVAÇÃO/JUSTIFICATIVA

2.1. Há diversos sistemas na VALEC, tanto de terceiros quanto desenvolvidos internamente, que dependem do SQL Server. É necessário ter o suporte ativo para este SGBD, que inclui o fornecimento de *patches* corretivos, evolutivos e de segurança. Sem o licenciamento/suporte contratado, não se tem a garantia de correção de erros nem apoio técnico especializado para solução de problemas que possam surgir, afetando os usuários dos sistemas e, por consequência, a missão da VALEC.

2.2. Os sistemas que usavam o SGBD Oracle estão em fase de finalização de migração para SQL Server. Após o fim da conversão, as aplicações 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 para continuar funcionando.

2.3. 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 e melhorias de desempenho. Destaca-se aqui algumas características da última versão do SGBD:

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

2.3.2. 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;

2.3.3. Encriptação com chaves criptográficas (AlwaysEncrypted with secure encrypted keys). O SQL Server agora pode encriptar porções de memória para trabalhar com colunas encriptadas sem expor os dados a outros processos ou para administradores;

2.3.4. 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;

2.3.5. 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;

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

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

2.3.8. 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.

2.4. Ainda, com o advento do sistema DTe (Documento de Transporte Eletrônico), faz-se necessário o correto dimensionamento da quantidade de cores licenciados 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 durante o período que aplicação funcionar na infraestrutura *on-premisse* da Valec.

2.5. Resultados pretendidos:

2.6. Verificar a viabilidade da manutenção do sistema gerenciador de banco de dados atualmente utilizado pela Valec.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. Identificação das necessidades de negócio

3.1.1. Os requisitos de negócio são aqueles que independem de características tecnológicas e que definem as necessidades e os aspectos funcionais da Solução de Tecnologia da Informação.

3.1.2. As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição da solução mais adequadas a tais objetivos organizacionais, conforme relação a seguir:

3.1.2.1. Possibilitar o acesso aos diversos dados utilizados amplamente pela Valec, mantê-los com segurança e integridade, permitir seu compartilhamento quando necessário e resguardar seu sigilo;

3.1.2.2. Ter acesso direto, através de consultas às bases de dados, cruzamento de dados, produção de trilhas de auditoria, etc., ou indireto através do acesso dos sistemas da casa aos bancos de dados.

3.2. Identificação das necessidades tecnológicas

3.2.1. As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0) com adaptações, descrevem as características de uma solução que atende aos requisitos do negócio, detalhados após a realização de uma análise mais aprofundada. Dentre os requisitos da solução de tecnologia, são descritos:

3.2.1.1. Os requisitos funcionais, aqueles que descrevem capacidades que a solução será capaz de executar em termos de comportamentos e operações – ações ou respostas específicas de aplicativos ou componentes de tecnologia da informação,

3.2.1.2. Os requisitos não funcionais, aqueles que capturam condições que não se relacionam diretamente ao comportamento ou funcionalidade da solução, mas descrevem condições ambientais sob as quais a solução deve permanecer efetiva, ou qualidades que os sistemas precisam possuir. Também são conhecidos como requisitos de qualidade ou suplementares. Podem incluir requisitos relacionados à capacidade, velocidade, segurança, disponibilidade, arquitetura da informação e apresentação da interface com o usuário, e

3.2.1.3. Os requisitos de transição, aqueles que descrevem capacidades que a solução deve possuir com o objetivo de facilitar a transição do estado atual da organização para um estado futuro desejado, mas que não serão mais necessárias uma vez concluída a transição. São diferenciados dos outros tipos de requisitos porque são sempre temporários por natureza e porque não podem ser desenvolvidos até que ambas as soluções, a nova e a existente, sejam definidas.

3.2.2. Nesse sentido, a presente seção descreve os macro requisitos tecnológicos considerados para fins de identificação e definição da solução mais adequada, conforme relação a seguir:

3.2.2.1. Atendimento às características essenciais a uma plataforma robusta de bancos de dados, tais como controle de redundância, controle de acesso aos dados, garantia de restrições de integridade e controle de recuperação a falhas;

3.2.2.2. Garantia de acesso imediato aos dados existentes nas bases de dados atuais por parte das aplicações já existentes na casa, em sua maioria desenvolvidas utilizando tecnologias Java e Microsoft, sem a necessidade de correções e/ou modificações nas aplicações citadas;

3.2.2.3. 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”;

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

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

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

3.3. Demais requisitos necessários e suficientes à escolha da solução de TIC

3.3.1. Além dos requisitos de negócio e tecnológicos, a presente seção destaca aqueles que devem ser considerados ao longo do planejamento da contratação para se assegurar o alcance aos objetivos pretendidos com a aquisição. O SGBD deve atender, pois, os seguintes requisitos:

3.3.1.1. Estar em conformidade com a LGPD;

3.3.1.2. Poder rodar em Windows Servers e Linux;

3.3.1.3. Operar com dados estruturados e não estruturados;

3.3.1.4. Ter documentação sempre atualizada e disponível;

3.3.1.5. Permitir encriptação;

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

3.3.1.7. Permitir codificação UTF-8 de caracteres;

3.3.1.8. Permitir expansão ilimitada de memória;

3.3.1.9. Permitir virtualização de dados;

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

3.3.1.11. Permitir classificação de dados;

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

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

3.3.1.14. Permitir segurança a nível de registro;

3.3.1.15. Mascaramento de dados;

3.3.1.16. Particionamento de tabelas e índices.

4. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

4.1. Após reestruturação dos SGBD na infraestrutura da Valec, definiu-se a necessidade de licenciar 24 *cores*, conforme demonstrado abaixo:

Servidor	Ambiente	*Cores*	Versão	Uso
BSB061	Produção	-	SQL Server 2017 Standard Edition	Share Point
BSB064	Produção	-	SQL Server 2017 Standard Edition	System Center Configuration Manager
BSB007	Produção	8	SQL Server 2017 Enterprise Edition	Novo ambiente em cluster
BSB008	Produção	8	SQL Server 2017 Enterprise Edition	SIGA, SIGEN , Assyst e aplicações migradas do Oracle
BSB066	Produção	2	SQL Server 2017 Enterprise Edition	Microsoft SQL Report Services - Interno
BSB067	Homologação	6	SQL Server 2017 Enterprise Edition	Servidor para homologação de mudanças
	Total	24		

4.2. Baseado na tabela anterior foi identificada a necessidade de 12 licenças SQL Enterprise (QLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic), que equivalem a concessão de 24 cores, pois essa é a quantidade atual de núcleos/cores dos servidores virtuais 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.

4.3. 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 (16), Homologação (6), Report Server (2), e futura utilização de instância de desenvolvimento (4) considerando a contratação da fabrica de software.

4.4. Note-se que o ambiente de desenvolvimento dispensa licenciamento, por isso não foi contabilizado.

5. ANÁLISE E IDENTIFICAÇÃO DE SOLUÇÕES DE MERCADO

5.1. Considerando o estudo de mercado anterior identificou-se as soluções a seguir que se apresentam como potenciais:

Id	Solução
1	Manutenção das licenças Microsoft SQL Server

2	Adoção de solução de software livre para banco de dados
3	Contratação de licença de outro software gerenciador de banco de dados

5.1.1. **Solução 1 -** Manutenção das licenças Microsoft SQL Server

5.1.1.1. Descrição da solução: Contratação/renovação das licenças atualmente em uso do Microsoft SQL Server para as instâncias já em uso dos bancos de dados da Valec.

5.1.1.2. Vantagens/Desvantagens da solução:

Vantagens	Desvantagens
- Manutenção do ambiente de banco de dados atualmente em produção na Valec, eliminando necessidade de qualquer tipo de adequação, como migrações de dados entre bancos;	- Apesar de reduzido, ainda há um custo;
- Manutenção das aplicações existentes na Valec, entre outros, eliminando necessidade de quaisquer adequações/modificações nas mesmas;	- Diminuição da competitividade na licitação;
- Manutenção das rotinas hoje executadas pelos usuários da Valec, sem necessidade de retrabalho e/ou mudança em qualquer tipo de processo existente;	
- Redução de custos com treinamentos básicos aos administradores de banco de dados da Valec;	
- Suporte à solução garantido pelo fabricante.	
- Robustez e ferramentas administrativas que auxiliam o tratamento dos dados.	

5.1.2. **Solução 2 - Adoção de solução de software livre para banco de dados.**

5.1.2.1. Descrição da solução: Adoção de plataforma de SGBD livre, provido pela comunidade de software livre.

5.1.2.2. Vantagens/Desvantagens da solução:

Vantagens	Desvantagens
- Sem custo de licenciamento	- Necessidade de migração das bases de dados atuais para o novo SGBD;
- Fácil administração (para ambientes não clusterizados);	- Necessidade de adequação das aplicações utilizadas na Valec para a correta utilização do novo SGBD;
- Boa documentação (comunidade e fabricante);	- Necessidade de modificação de qualquer tipo de processo de trabalho existente na Valec que necessite de acesso direto aos bancos de dados existentes na casa;
- Possui compatibilidade com a maioria das aplicações;	- Possível dificuldade de integração entre o novo SGBD e outras plataformas existentes na casa e que dele dependam;
	- Necessidade de adequação de processos de backup já existentes e em funcionamento na Valec;
	- Necessidade de treinamentos a serem conferidos aos administradores de banco de dados da Valec para utilização do novo SGBD;
	- Não há garantia de suporte, já que o mesmo é obtido através da comunidade de software livre;
	- Baixo nível de segurança;
	- Poucas ferramentas administrativas para gerenciar o banco de dados;
	- Degradação de performance com banco de dados de grande robustez ou volumes transacionais elevados;
	- Baixa velocidade nas execuções dos Backup;
	- Maior dificuldade para depurar erros internos;

5.1.3. **Solução 3 - Contratação de licença de outro software gerenciador de banco de dados.**

5.1.3.1. Adoção de plataforma de outro fornecedor, diferente da atualmente utilizada na Valec.

5.1.3.2. Vantagens/desvantagens da solução como um todo:

Vantagens	Desvantagens
- Suporte à solução	- Necessidade de migração das bases de dados atuais para o novo SGBD;

garantido pelo fabricante;	
- Maior competitividade na licitação;	- Necessidade de adequação das aplicações utilizadas na Valec para a correta utilização do novo SGBD;
	- Indisponibilidade, acidental ou programada, dos bancos de dados existentes, com reflexo consequente nos sistemas e serviços que utilizem os referidos bancos;
	- Possível dificuldade de integração entre o novo SGBD e outras plataformas existentes na casa e que dele dependam;
	- Necessidade de modificação de qualquer tipo de processo de trabalho existente na Valec que necessite de acesso direto aos bancos de dados existentes na casa;
	- Necessidade de adequação de processos de backup já existentes e em funcionamento na Valec;
	- Necessidade de treinamentos a serem conferidos aos administradores de banco de dados da Valec para utilização do novo SGBD;
	- Maior custo agregado para implantação da solução.

5.2. Avaliação das soluções identificadas frente aos requisitos:

Requisitos	**Solução 1 - Manutenção das licenças Microsoft SQL Server**	**Solução 2 - Adoção de solução de software livre para banco de dados.**	**Solução 3 - Contratação de licença de software semelhante de outro fornecedor.**
Manutenibilidade	Atende	Atende	Atende
Acesso imediato das aplicações	Atende	Não atende	Não atende
Backup	Atende	Atende parcialmente	Atende
Replicação de dados	Atende	Atende	Atende parcialmente
Alta disponibilidade	Atende	Atende parcialmente	Atende parcialmente
Suporte	Atende	Não atende	Atende

5.3. **Análise comparativa de soluções**

5.3.1. Examina-se nesta seção, para cada solução, os aspectos previstos na IN SGD-ME nº 01/2019 que devem ser avaliados em uma contratação de TIC.

Requisito	Solução	Sim	Não	Não se Aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1	X		
	2	X		
	3	X		
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de Software)	1		X	
	2		X	
	3		X	
A solução é composta por software livre ou software público? (quando se tratar de Software)	1		X	
	2		X	
	3	X		
A solução é aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo ePing, eMag, e PWG?	1			X
	2			X
	3			X
A solução é aderente às regulamentações da ICP- Brasil? (quando houver necessidade de certificação digital)	1			X
	2			X
	3			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	1			X
	2			X
	3			X

(quando o objetivo da solução abranger documentos arquivísticos)				

6. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

6.1. A Solução 2 mostrou-se inviável por:

- não ter atendido o requisitos Acesso imediato das aplicações, pois, se adotada, implicaria em conversão do código das aplicações a fim de adaptá-las ao novo SGBD e
- não ter atendido o requisito Suporte, que deve ser contratado separadamente.

6.2. A Solução 3 mostrou-se inviável por:

- não atender o requisito de Acesso imediato das aplicações, enquadrando-se na mesma situação da solução 2;
- atender só parcialmente o requisito de Replicação de dados;
- atender só parcialmente o requisito de Alta disponibilidade.

7. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

7.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 4.1 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

8. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

8.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 4.2 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

9. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

9.1. O Microsoft SQL Server é um software do tipo “sistema gerenciador de banco de dados” (SGBD) projetado para gerenciar o acesso, a persistência, a manipulação e a organização dos dados nele armazenados. Ele permite diversos tipos de consulta ou cruzamento de dados, diretamente ou através de aplicações desenvolvidas pelas equipes de TI, necessária à compleição da missão da Valec.

10. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

10.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 4.3 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

11. JUSTIFICATIVAS PARA PARCELAMENTO OU NÃO DA SOLUÇÃO

11.1. Não se aplica tendo em vista tratar-se de um produto único.

12. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

12.1. Não se aplica.

13. PROVIDÊNCIAS A SEREM ADOTADAS ANTES DA CONTRATAÇÃO

13.1. Como o ambiente atual da Valec já possui o licenciamento da referida ferramenta, não há providências prévias a serem adotadas.

14. ANÁLISE DE CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

14.1. Conforme Termo de Referência SEI 3734548, itens 5.6 e 8.

15. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS DE TRATAMENTO

15.1. Conforme Termo de Referência SEI 3734548, itens 5.6 e 8.

16. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

16.1. A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

16.2. Nesse sentido, o planejamento em tela almeja os seguintes resultados:

- Economia no valor da aquisição;
- Eficiência com a redução do custo administrativo em função da redução da fragmentação de processos licitatórios;
- Efetividade com a padronização dos produtos e oferta de uma solução que objetiva maior produtividade;
- Eficácia com o atendimento das necessidades tecnológicas e de negócio da Valec.

16.3. A Valec utiliza o banco de dados Microsoft SQL Server há mais de 10 anos, seja em processos de carga, ETL’s, trilhas de auditoria ou consultas AD-HOC e, obviamente, fornecimento dos dados aos sistemas do órgão.

16.4. Dessa forma, a expertise dos servidores, tanto das equipes de TI, quanto das equipes finalísticas, é muito grande. Cabe destacar os seguintes pontos:

a) Redução de riscos de continuidade pela manutenção de SGBD já em uso pela Valec;

b) Manutenção dos processos de acesso ao banco atualmente em uso;

c) Analistas já treinados e com expertise na utilização da plataforma;

d) Inexistência de esforço e adaptação para substituição das soluções;

e) Custo da renovação das licenças;

16.5. Tendo em vista as maiores vantagens e o cumprimento dos requisitos essenciais para total atendimento da demanda, optou-se pela Solução 1: Manutenção das licenças Microsoft SQL Server, sendo a descrição padrão da Microsoft o termo SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic, SKU 7JQ-00341.

16.6. A análise atende ao critério de redução dos custos totais para o atendimento de necessidades por bens e serviços, englobando eventuais despesas com contratos e demais gastos necessários ao atendimento das necessidades e oportunidades de padronização e integração de bens e serviços.

16.7. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis.

16.8. Considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente **VIÁVEL.**

17. APROVAÇÃO E ASSINATURA

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

17.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	**INTEGRANTE REQUISITANTE**
_____ **JOSE AUGUSTO MEIRA DA ROCHA** **Matrícula/SIAPE: 2340257**	_____ **ROBÉRIO XIMENES DE SABÓIA** **Matrícula/SIAPE: 1990222**
AUTORIDADE MÁXIMA DA ÁREA DE TIC **(OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)**	
_____ **JORGE LUIS DA SILVA LUSTOSA** **Matrícula/SIAPE: 1105206**	

Documento assinado eletronicamente por **José Augusto Meira da Rocha**, **Integrante Técnico**, em 01/03/2021, às 15:56, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Sabóia**, **Integrante Requisitante**, em 01/03/2021, às 15:59, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Jorge Luis da Silva Lustosa**, **Superintendente**, em 01/03/2021, às 19:07, conforme horário oficial de Brasília, com fundamento no art. 3°, 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 **3693150** e o código CRC **17FC4EEF**.

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

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

Estudo Técnico Preliminar da Contratação/SUPTI-VALEC/DIRAF-VALEC-VALEC

Brasília, 07 de fevereiro de 2021.

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
07/02/2020	1.0	Finalização da primeira versão do documento	Cláudio Amorim de Sousa
27/02/2020	1.1	Revisão prévia de envio ao setor de licitações	Jorge Luis da Silva Lustosa

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1. INTRODUÇÃO

1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda SEI 3781122, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. Durante o Estudo Técnico Preliminar, diversos aspectos devem ser levantados para que os gestores certifiquem-se de que existe uma necessidade de negócio claramente definida, há condições de atendê-la, os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente.

1.3. O objeto do estudo é a contratação de solução **CASB (Cloud Access Security Broker)** que atendam de forma ampla às demandas da Valec Engenharia, Construções e Ferrovias S.A.

2. MOTIVAÇÃO/JUSTIFICATIVA

2.1. A infraestrutura da VALEC atualmente, de acordo com a Gerência de Infraestrutura (GEINF/SUPTI/DIRAF) possui 70% dos ativos da informação alocados em datacenter na Sede, demais serviços encontram-se alocados na nuvem.

2.2. Além da necessidade de utilização de software de segurança a fim de atender a proposta das duas infraestruturas, on-premises e na nuvem (IaaS), através de cessão temporária de direito de uso (subscrição) para endpoints em infraestrutura *on-premises* (local) usando a tecnologia Next-Generation Antivírus (ETP 3715636), há a necessidade de proteção dos ativos da informação e aplicações na nuvem através da solução CASB contra ameaças provenientes de dispositivos corporativos (gerenciados) e pessoais (não-gerenciados), utilizando-se recursos de auditoria de acessos na infraestrutura da nuvem (IaaS).

2.3. A reforma trabalhista ocorrida em julho de 2017, através da LEI N. 13.467, que define a nova modalidade de trabalho, do CAPÍTULO II-A - "DO TELETRABALHO", foi regulamentada proporcionando tanto para o trabalhador quanto para as empresas, segurança trabalhista. Somado-se a fatídica pandemia iniciada em dezembro 2019, com reflexo no Brasil e no mundo, essas situações contribuíram para a difusão desta nova forma de trabalho.

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

2.5. A infraestrutura em nuvem (IaaS) é um novo conceito para a VALEC, onde alguns serviços encontram-se dispostos e em operação, a exemplo, a suite Office 365 (SaaS) disposto 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.

2.6. A solução CASB (Cloud Access Security Broker) 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 deste estudo.

2.7. Assim como a proteção dos ativos da informação da VALEC, a auditoria no acesso aos 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 2.5, sendo criterioso a auditoria na gestão de identidade, assim como a gestão de controle de acesso contra vazamento de dados (DLP) através de políticas configuráveis na solução em consonância com a LGPD.

2.8. A LGPD promulgada através da Lei 13709 de 14 de agosto de 2018, demonstra a necessidade de tratamento e privacidade dos dados pessoais, definindo mecanismos de coleta e tratamento de dados através de aplicação de governança e indicação de de atores para tratamento dos dados como: operador, controlador, e encarregado.

2.9. Desta forma, com intuito de tratar os dados, faz-se necessário aquisição deste tipo de ferramenta que auxilie nesta tarefa, identificando os dados sensíveis e possibilitado através da configuração de políticas no software a classificações dos dados sensíveis, como exemplo: CPF, RG, número de cartões de crédito, evitando assim o vazamento de dados, como por exemplo, no uso de aplicativos da suite Office 365 utilizados pelo usuário.

2.10. A ferramenta CASB através do recurso de proteção contra vazamento de dados (DLP) auxilia diretamente na auditoria e na gestão de cibersegurança da Estatal, sendo um ferramental poderoso para a proteção e tratamento de dados pessoais no âmbito da VALEC.

2.11. Em resumo, estas Instruções têm como finalidade:

I - Propiciar proteção aos ativos da informação e aplicações na nuvem para a regra de negócios da VALEC contra vazamento de dados (DLP);

II - Propiciar mecanismo para auditoria no acesso aos ativos da informação da VALEC dispostos na infraestrutura em nuvem (IaaS) como serviço (SaaS).

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. Identificação das necessidades de negócio

3.1.1. A incidência de ataques contra órgãos e empresas públicas no âmbito da administração federal se tornou incisiva e recorrente nos últimos meses de 2020, onde os hackers exploraram diversas técnicas de invasão e disseminação, em busca de informações, motivados por viés político ou partidário, ou mesmo por disputas de regimes entre potências econômicas, como casos recentes aos ataques de hackers contra o STJ e TSE (Ataques de hackers STJ e TSE, acesso em 26/02/2021), ocorridos nos meses de novembro e dezembro de 2020, assim como o ataque ocorrido por grupo hacker da Rússia contra as agências norte americanas (Ataque hacker Russo às Agências dos EUA, acesso em 26/02/2021, através da contaminação de software de administração de redes de computadores, Solarwinds, ocorrido em dezembro de 2020.

3.1.2. As técnicas de ataques e exploração de vulnerabilidades evoluíram com o passar dos anos, antigas técnicas de ataques do tipo *Smurf attacks, Ping of Death (PoD),* que tratam de tentativas de exaustão da rede e dos sistemas operacionais não são mais utilizadas em detrimento de técnicas recompensatórias, como exemplo, malwares do tipo *ransomware*, e sequestro de dados para mineração de ativos monetários, as *crypto moedas* (conceito blockchain) utilizando ataques do tipo *cross-site scripting (XSS)*.

3.1.3. O conceito de estrutura organizacional tornou-se complexo, visto que, o cenário de escritórios físicos, assim como alocação de postos de trabalho, tornam-se cada vez mais dispendiosos, levando as entidades públicas e privadas a repensarem no modelo de negócio quanto à disposição de espaços físicos, tendendo cada vez mais na concessão de conectividade remota, seja por termos de empréstimo de dispositivos corporativos, como exemplo notebooks, seja por concessão de sessão remota através de dispositivos BYOD - notebooks particulares, smartphones ou tablets.

3.1.4. Para os ativos da informação (dados e serviços) dispostos na nuvem, como exemplo a suite do Office365, o acesso pode ser feito através de qualquer dispositivo gerenciável ou não. Independentemente do dispositivo ser corporativo ou pessoal, é necessário aplicação de segunda camada, atribuída a nuvem, para proteção dos ativos da informação, através da solução CASB.

3.1.5. 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 na nuvem através de software de segurança do tipo CASB, estabelecendo uma camada de proteção ativa para os ativos da informação da VALEC na nuvem.

3.1.6. Demais requisitos de negócio estão relacionados a auditoria para estes acessos, fazendo-se necessário recursos ferramentais dispostos nesta mesma solução, CASB, a fim de contribuir para gestão de identidade, de gestão de controle de acessos, gestão de informações protegidas (gestão de segurança de privacidade de informações), auxiliando na formação de uma Gestão Cibernética para a VALEC, em acordo com a LGPD.

3.2. Identificação das necessidades tecnológicas

3.2.1. Com a implementação e manutenção ativa do software do tipo Endpoint Next-Generation Anti-malware através de agente, estabelece-se a proteção no parque tecnológico da VALEC contra exploração de ataques laterais para as estações de trabalho e servidores, porém há a necessidade de proteção no sentido norte-sul para acesso aos ativos da informação da VALEC dispostos na nuvem.

3.2.2. A camada norte-sul atualmente está desprotegida, sendo necessária sua proteção e consequente auditoria, em vista da nova modalidade de acesso dos usuários de alguns aos serviços distribuídos da VALEC alocados em nuvem, como exemplo: a suite Office 365 (SaaS) disposto 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.

3.2.3. A proposta deste ETP, é delinear através de análise técnica a interpretação das novas tendências de ataques e vazamento de dados (DLP) na infra de nuvem (IaaS), definindo mecanismo de proteção mais indicados para proteção ativa para acesso aos ativos da informação da VALEC contra malwares e vazamento de dados, incluindo mecanismo de auditoria.

3.2.4. Desta forma, propõe-se a utilização da solução CASB, através de software no formato de serviço na nuvem (SaaS), para atender a proteção ativa dos ativos da informação da VALEC contra ameaças de malwares provenientes de dispositivos corporativos (gerenciados) ou pessoais (não-gerenciados), proteção contra vazamento de dados (DLP), e disposição de uso de ferramenta de auditoria inclusa na solução para acessos com integração do serviço de gerência e identidade dos usuários da VALEC na nuvem, *Azure Active Directory*.

3.2.5. A solução provê, visibilidade de aplicações utilizadas nos dispositivos que conectam-se aos serviços da nuvem, contendo painel dashboard das aplicações mais utilizadas, informações de dispositivos e usuários conectados, volume de tráfego, tempo de uso de cada aplicação na nuvem, e classificação do risco do uso, localização geográfica, auditoria de acessos, edição, cópia do arquivo e conteúdo, exclusão, download, upload.

3.3. Do contrato atual

3.3.1. Não há contrato para proteção de dados e vazamento (DLP) para os ativos da informação na nuvem.

3.3.2. Não há contrato para auditoria na proteção de dados e vazamento (DLP) para os serviços (SaaS) da VALEC dispostos na nuvem. MS Office 365 e ferramentas colaborativas, assim como futura utilização do serviço de gerência e identidade dos usuários da VALEC na nuvem, *Azure Active Directory*.

3.3.3. Há contrato vigente (008-18 - Omega Tecnologia) para auditoria, controle e gerência de permissionamento dos serviços em ambiente local (on-premises) para os serviços do AD (Microsoft Active Directory), de servidor de Arquivos (Microsoft File Server) e de sistema de correio eletrônico (Microsoft Exchange Server). O contrato tem vigência até 07 de março de 2021. As licenças se baseiam em usuário e são perpétuas. Ocorrerá perda de suporte.

3.3.4. O serviço de e-mail atual trabalha 100% na nuvem, estando descoberto pelo contrato vigente a auditoria para este serviço, devido a limitação da ferramenta que opera somente na infraestrutura local (on-premises).

3.3.5. O serviço do AD local (on-premises) está coberto pela solução Varonis (Omega Tecnologia), porém este serviço será migrado para a nuvem, com nova denominação, "Azure Active Directory", no momento que for adquirida ferramenta de suíte de escritório Microsoft 365, que o contemplará no pacote.

3.3.6. Assim como o AD local, o servidor de arquivos também está contemplado pela solução Varonis de forma local (on-premises), porém, a migração de parte do servidor de arquivos para a nuvem já fora iniciada com algumas unidades, ex. SUPTI, já utilizando os arquivos diretamente na nuvem através de ferramentas colaborativas da suíte Office 365: Teams, SharePoint.

3.3.7. Devido a tendência de contratações por software como serviço na nuvem (SaaS), objeto de estudo deste ETP, com a migração integral do AD e parcial do servidor de arquivos para a nuvem, a ferramenta de auditoria Varonis terá efetividade somente na estrutura local (on-premises), onde sua licença é perpétua.

3.4. **Quadro resumo do objeto de estudo deste ETP e proposta para contratação de software de segurança CASB:**

1	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);
2	Criar camada de proteção contra malwares na infraestrutura de nuvem para proteger os ativos da informação da VALEC a fim de garantir a integridade, disponibilidade e confidencialidade;
3	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;
4	Aplicar mecanismos de proteção contra vazamentos de dados (DLP) na nuvem (IaaS);
5	Aplicar mecanismos de auditoria através de ferramenta integrada a solução CASB no acesso as informações dispostas na nuvem em acordo com a LGPD.

4. CARACTERÍSTICAS GERAIS DA SOLUÇÃO CASB PARA PROTEÇÃO CONTRA AMEAÇAS DE MALWARES, VAZAMENTO DE DADOS (DLP), E AUDITORIA - NA NUVEM (SAAS)

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

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

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

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

4.5. 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-sancionadas;

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

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

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

4.9. 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;*

4.10. 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);

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

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

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

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

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

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

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

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

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

4.20. 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;

4.21. 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).

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

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

4.24. 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);

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

4.26. 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;

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

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

4.29. Classificação de “dados sensíveis” automatizada do conteúdo que está sendo carregado e armazenado em aplicativos e serviços em nuvem;

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

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

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

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

4.34. 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;

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

4.36. 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;

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

4.38. 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;

4.39. 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.

4.40. 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;

4.41. 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;

4.42. 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.

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

4.44. 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.

4.45. 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;

4.46. 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;

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

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

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

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

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

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

4.53. 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.

4.54. 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.

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

4.56. 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;

4.57. 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;

4.58. Deve possuir multifator de Autenticação;

4.59. 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;

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

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

5. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

5.1. A presente sessão contém o registro do quantitativo estimado de itens para a composição da solução a ser contratada, de forma detalhada, e justificada, inclusive quanto à forma de cálculo. Busca-se descrever também os métodos, metodologias e técnicas de estimativas que foram utilizados, nos termos do inciso I do art. 11 da IN SGD-ME n. 01/2019.

5.2. A principal análise é a quantidade de servidores dispostos na infra da VALEC e de forma remota (teletrabalho) que irão utilizar tanto dispositivos corporativos (gerenciados), quanto dispositivos pessoais (não-gerenciados).

5.3. Considerando a difusão e adesão do teletrabalho na empresa, o licenciamento Microsoft para suítes de escritório contempla o uso por usuário para até 15 (quinze) dispositivos: 5 (cinco) computadores, 5 (cinco) tablets, e 5 (cinco) smartphones.

5.4. A proteção ativa contra vazamento de dados (DLP) e auditoria na nuvem a ser atendida pela solução CASB - Cloud Access Security Broker, considera a proteção licenciada por usuário independente do quantitativo de dispositivos simultâneos estejam acessando os dados da Valec na nuvem.

5.5. Com o propósito de checar a quantidade de usuários ativos na VALEC foi realizada pesquisa na base de dados dos usuários da rede (serviço de diretório-autenticação).

5.6. Com o auxílio da ferramenta Power Bi, foram coletadas as informações necessárias para o quantitativo de usuários da rede conforme ilustra a imagem abaixo:

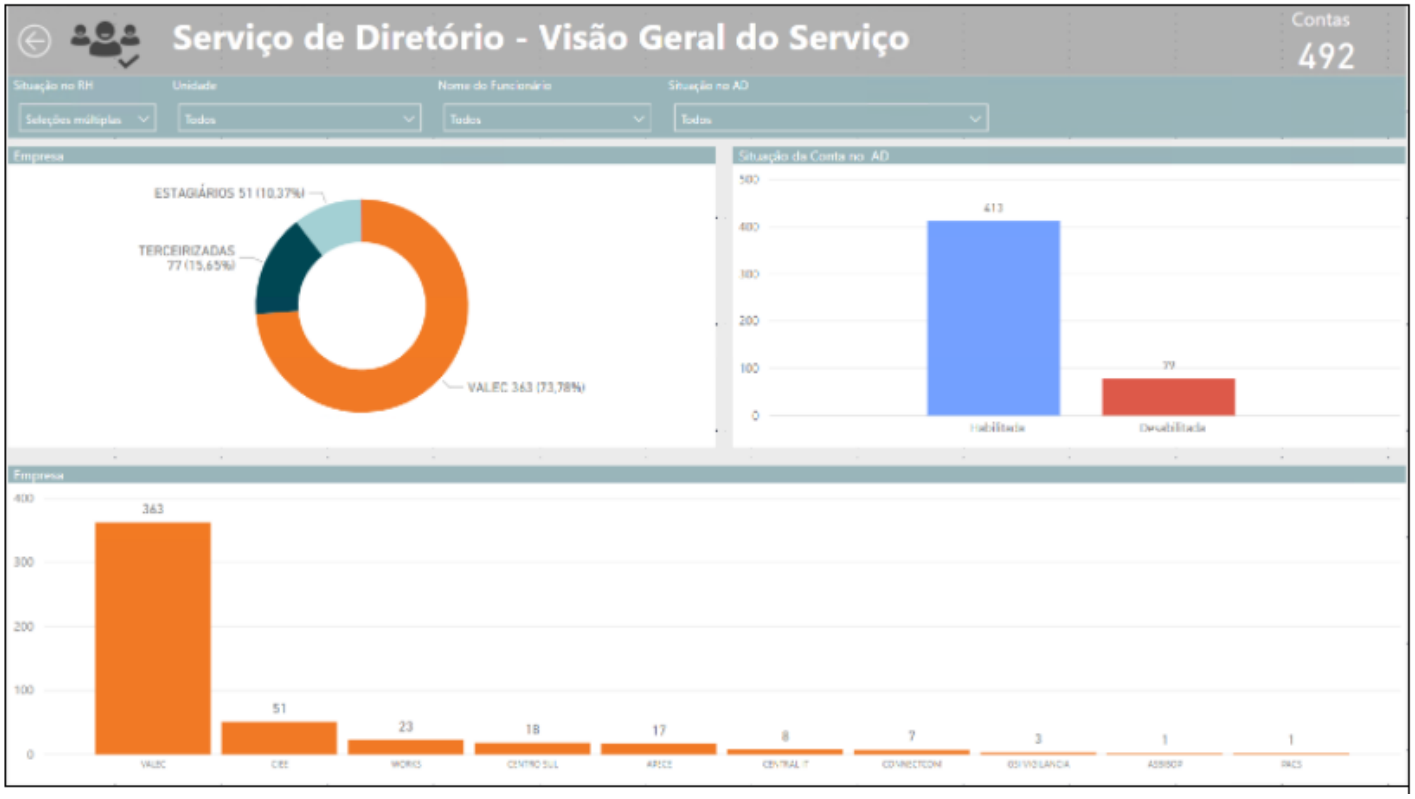


Fig. 01 - Painel de Usuários - Serviço de diretório - Visão Geral do Serviço (Extraído em 12/02/21) *Considerando o cenário atual com 79 contas desabilitadas.

5.7. No primeiro gráfico podemos observar que temos três tipos de usuários na empresa:

5.8. Usuários Valec: Compreendem servidores do quadro da VALEC, RFFSA, GEIPOT. Usuários que estão ativos, e não cedidos a outros órgãos. Estes usuários fazem uso dos computadores da empresa para execução diária de suas atividades laborais.

5.9. Usuários Estagiários: São estudantes de nível médio e superior. Cabe salientar que o contrato com o CIEE foi encerrado em dezembro último. Porém, na extração da informação do quantitativo, há época existiam 51 estagiários distribuídos nas 11 superintendências e 4 assessorias executando atividades administrativas de baixa complexidade e com prazo flexível para suas entregas, uma vez que são aprendizes. Há espectativa que seja celebrado novo contrato no primeiro semestre de 2021, atingindo o mesmo quantitativo.

5.10. Usuários Terceirizados: Compreende usuários de empresas com contratos ativos com a Valec, que prestam serviço em suas dependências, sejam elas obras ou dentro dos escritórios da Valec. Cabe esclarecer que a contratação desta solução não abrange a disponibilização de licenças ou computadores a empresas terceirizadas, uma vez que se tratam de recursos inerentes a prestação de serviço. Exceto em casos onde há previsão contratual de uso de recursos da contratante, como por exemplo os serviços de recepção, portaria ou suporte técnico, onde é desejável que a empresa use os mesmos recursos disponibilizados aos usuários com o propósito de compreender a perspectiva do usuário.

5.11. Nos gráficos subsequentes podemos observar como estes 3 grupos estão distribuídos na empresa. Cabe notar que neste painel o filtro utilizado foi da atual situação dos usuários e a empresa, excluindo usuários cedidos e terceirizados não habilitados ao uso do serviço. Por conta disto o total foi reduzido para 444 pessoas.

5.12. Da incorporação da EPL a Valec - Conforme matéria veiculada nos meios de comunicação conforme a publicação (3790025), onde o Ministério da Infraestrutura divulga o plano de incorporação da Empresa de Planejamento e Logística S.A. prevista para ocorrer no primeiro semestre de 2021. Cabe observar que foi celebrado o contrato de consultoria para estruturação do projeto, entre a Valec e a Empresa Falconi(51402.101308/2020-31), para estruturação técnica do projeto de incorporação. Até o momento ainda não foi possível estabelecer de maneira precisa o quantitativo final, logo foi considerado o quantitativo de funcionários efetivos daquela empresa, totalizando 121 pessoas, onde somando-se ao quadro de extração de dados da figura 01, têm-se o quantitativo final de 565 de usuários que serão cobertos pelas licenças a serem contratadas.

5.13. Baseado no estudo acima para atender a VALEC, estima-se a contratação dos seguintes itens, conforme tabela a seguir:

Item	Descrição	Qtd	Período
01	Fornecimento, instalação, configuração, manutenção e garantia de funcionamento de software de segurança do tipo CASB para proteção de dados e aplicativos em nuvem (IaaS) contra ameaças Anti-Malware, vazamento de dados (DLP), e auditoria. Licença por usuário.	565	36 meses

6. ANÁLISE DE SOLUÇÕES

6.1. Considerando a IN 01 DE 2019 que instrui a contratação de serviços na nuvem e considerando o PDTI 2019/2021 nota-se uma tendência por contratações de serviços na nuvem (SaaS), situação real e iminente também para outros serviços consonante com a

atual necessidade para aquisição de software de segurança CASB voltado para este tipo de infraestrutura.

6.2. A camada norte-sul atualmente está desprotegida, sendo necessária sua proteção e consequente auditoria, em vista da nova modalidade de acesso dos usuários de alguns aos serviços distribuídos da VALEC alocados em nuvem, como exemplo: a suíte Office 365 (SaaS) disposto 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.

6.3. A solução provê, visibilidade de aplicações utilizadas nos dispositivos que conectam-se aos serviços da nuvem, contendo painel dashboard das aplicações mais utilizadas, informações de dispositivos e usuários conectados, volume de tráfego, tempo de uso de cada aplicação na nuvem, e classificação do risco do uso, localização geográfica, auditoria de acessos, edição, cópia do arquivo e conteúdo, exclusão, download, upload.

6.4. A subscrição do tipo CASB (Cloud Access Security Broker) fará a proteção dos ativos da informação da VALEC na nuvem considerando os dispositivos do tipo *zero-trust (*não confiáveis), validando a sessão remota para estes, a partir de proteção na camada de aplicação, através de autorização (autenticação) do tipo SSO contendo políticas de utilização de uso, recursos e dados, com aplicabilidade de auditoria.

6.5. O acesso aos ativos da informação da VALEC na nuvem, podem por exemplo estar condicionadas ao tipo de dispositivo, ex. dispositivos corporativos da VALEC, notebooks, possuirão agente Endpoint Next-Generation Anti-malware instalado, tendo confiabilidade para upload de arquivos, oposto a dispositivos do tipo BYOD, considerados do tipo shadow IT (aplicações não homologadas pela TI) ou zero-trust (não-confiáveis).

6.6. Para a solução CASB, não foi identificado órgão que tenha iniciado contratação, acredita-se pelo fato de grande parte dos órgãos encontrarem-se em fase de planejamento para migração do serviços para a nuvem.

7. IDENTIFICAÇÃO DAS SOLUÇÕES

1	Solução de segurança do tipo CASB (SaaS) para proteção de dados e aplicações na nuvem contra ameaças Anti-Malware, vazamento de dados (DLP), e auditoria na nuvem. Broker (Proxy) posicionado na nuvem (SaaS).
2	Solução de segurança do tipo CASB (SaaS) para proteção de dados e aplicações na nuvem contra ameaças Anti-Malware, vazamento de dados (DLP), e auditoria na nuvem. Broker (Proxy) posicionado no ambiente local (on-premises).

7.1. Análise Comparativa de Soluções

7.1.1. Esta Gerência de Segurança da Informação GSINF/SUPTI/DIRAF, fez levantamento das principais soluções aplicáveis do tipo CASB para proteção dos ativos da informação e aplicações na nuvem, baseado nos seguintes fundamentos:

a) estudos das normas brasileiras e internacionais de segurança da informação, ISO 27001/27002/27005/17799;

b) da IN 01 de abril de 2019 do SGD;

c) das leis de proteção de dados LGPD e GDPR;

d) da tendência de uso das tecnologias de proteção;

e) da aplicabilidade da solução em órgãos do governo federal e estadual através de ETP's e contratações nos portais, SEI, ComprasNet, e Pesquisa de Preços;

f) da consulta de software de disponibilidade de software em sítios do portal de Software Público Brasileiro;

g) do contato realizado com fornecedores solicitando apresentação das soluções comercializadas;

7.2. Da solução 1 - Solução de segurança do tipo CASB (SaaS) para proteção de dados e aplicações na nuvem contra ameaças Anti-Malware, vazamento de dados (DLP), e auditoria na nuvem. Broker (Proxy) posicionado na nuvem (SaaS)

7.2.1. Do conceito CASB definido pelo Gartner: "**Cloud access security brokers (CASBs)** são pontos de aplicação de política de segurança locais (on-premises) ou baseados em nuvem, colocados entre os consumidores de serviços em nuvem e os provedores de serviços em nuvem para combinar e interpor políticas de segurança corporativa conforme os recursos baseados em nuvem são acessados. Os CASBs consolidam vários tipos de aplicação da política de segurança. Políticas de segurança, como exemplo, incluem autenticação, logon único, autorização, mapeamento de credencial, perfil de dispositivo, criptografia, tokenização, registro, alerta, detecção / prevenção de malware e assim por diante." Fonte: https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs [Acesso em 08/01/2021]

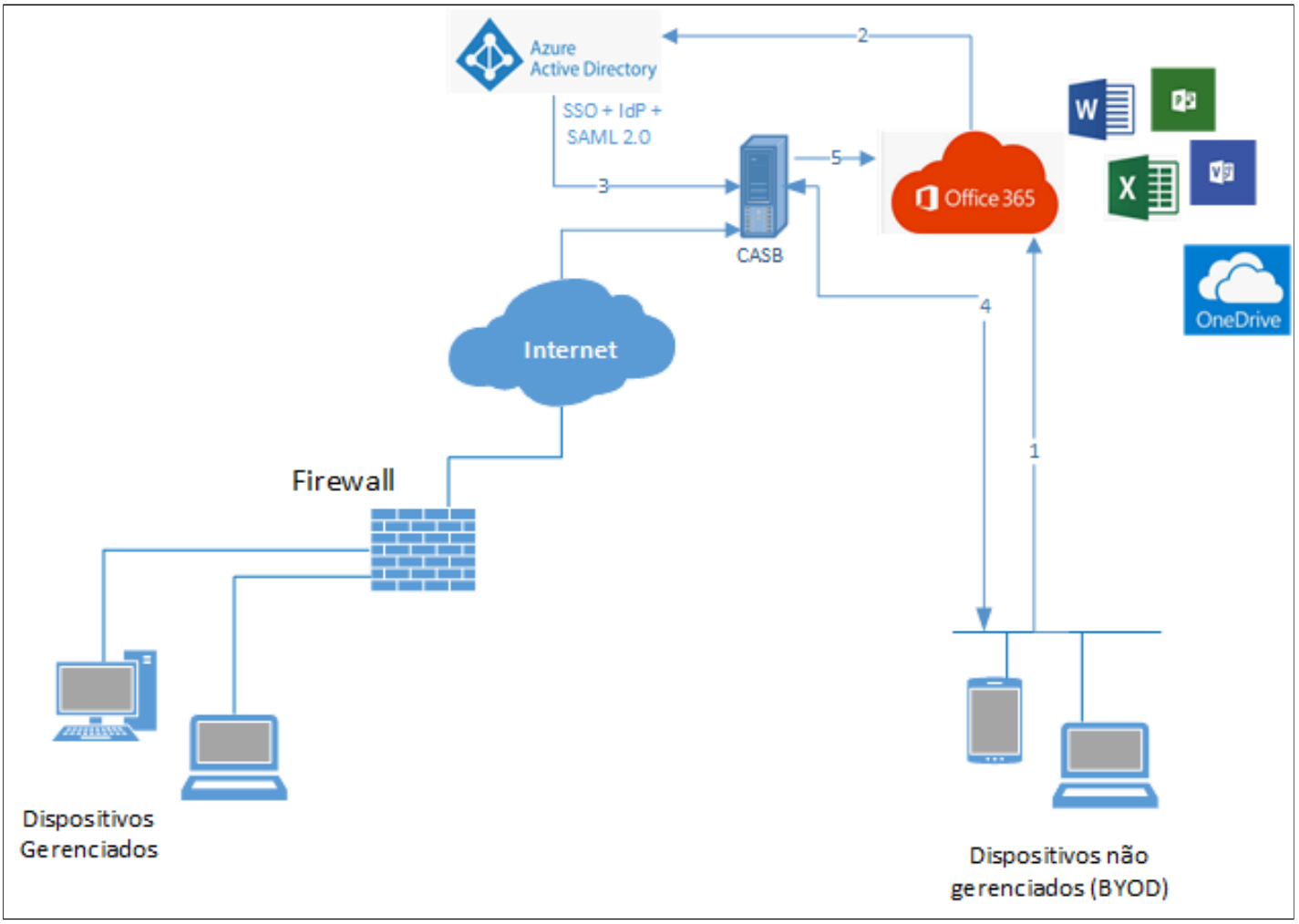


Fig. 02 - Topologia da solução CASB - Broker (Proxy) posicionado na nuvem (SaaS).

7.2.2. Na topologia acima o CASB, comumente referenciado como "*broker*", traduzindo: intermediário/agenciador/corretor, é um ativo a ser posicionado na nuvem do fabricante que faz a intermediação da sessão do usuário com dispositivo gerenciado ou não-gerenciado BYOD (celular, tablet, notebook) na autenticação, utilizando o protocolo IdP (identity provider) para validação e redirecionamento da conexão.

7.2.3. Desta forma, o CASB posicionado na nuvem (SaaS) consegue interceptar o tráfego monitorando as ações de acesso do dispositivo endpoint gerenciado e não-gerenciado (BYOD) aos arquivos e ativos da informação na nuvem através de políticas de controle editáveis (DLP) e pré-definidas dispostas na ferramenta, considerando o princípio da política de privacidade e proteção de dados pessoais da Estatal.

7.2.4. O usuário através de dispositivo gerenciado ou não-gerenciado, por exemplo, usando um notebook, ou celular, ao conectar-se no office 365 através da url, https://www.office.com/, hospedada pelo provedor de serviços Microsoft, este possui apontamento para servidor de identidade IdP (identity provider) apontando a autenticação para o Azure Active Directory (VALEC) que atua como autenticador do tipo SSO (single sign-on) através da interoperabilidade SAML 2.0 (Security Assertion Markup Language) encaminhando a requisição para o broker, CASB, que retorna ao usuário a autenticação, assim, o usuário acessaria o Office 365 na nuvem passando pelo broker, CASB, que detém as políticas e regras de acesso.

7.3. **Da solução 2 - Solução de segurança do tipo CASB (SaaS) para proteção de dados e aplicações na nuvem contra ameaças Anti-Malware, vazamento de dados (DLP), e auditoria na nuvem. Broker (Proxy) posicionado no ambiente local (on-premises)**

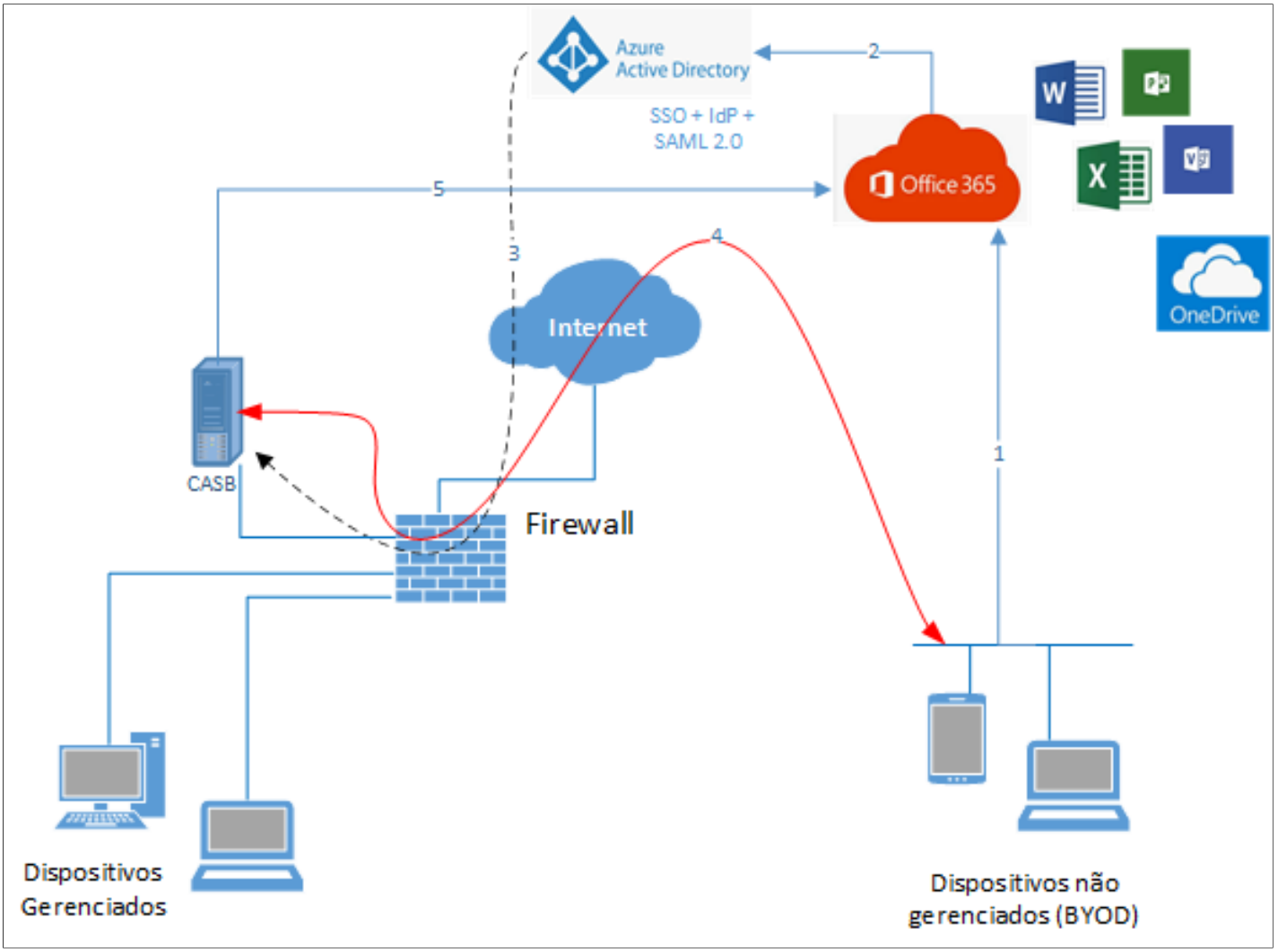


Fig. 03 - Topologia da solução CASB - Broker (Proxy) posicionado no ambiente local (on-premises).

7.3.1. Na topologia acima o CASB, está posicionado no ambiente do cliente, infra local (on-premises) da VALEC, fazendo a intermediação da sessão do usuário com dispositivo gerenciado ou não-gerenciado BYOD (celular, tablet, notebook) na autenticação, utilizando o protocolo IdP (identity provider) para validação e redirecionamento da conexão.

7.3.2. Desta forma, o CASB posicionado no ambiente do cliente (VALEC) consegue interceptar o tráfego monitorando as ações de acesso do dispositivo endpoint gerenciado e não-gerenciado (BYOD) aos arquivos e ativos da informação na nuvem através de políticas de controle editáveis (DLP) e pré-definidas dispostas na ferramenta, considerando o princípio da política de privacidade e proteção de dados pessoais da Estatal.

7.3.3. O usuário através de dispositivo gerenciado ou não-gerenciado, por exemplo, usando um notebook, ou celular, ao conectar-se no office 365 através da url, https://www.office.com/, hospedada pelo provedor de serviços Microsoft, este possui apontamento para servidor de identidade IdP (identity provider) apontando a autenticação para o Azure Active Directory (VALEC) que atua como autenticador do tipo SSO (single sign-on) através da interoperabilidade SAML 2.0 (Security Assertion Markup Language) encaminhando a requisição para o broker, CASB, que retorna ao usuário a autenticação, assim, o usuário acessaria o Office 365 na nuvem passando pelo broker, CASB, que detém as políticas e regras de acesso.

7.4. Abaixo segue quadro do Gartner demonstrando a evolução de maturidade e habilidade de execução de cada fabricante (*player*) para atendimento e desenvolvimento da solução CASB. O quadro é composto por 4 níveis: visionários (*visionaries*), estável (*niche*), desafiantes (*challengers*), e líderes (*leaders*):

Figure 1: Magic Quadrant for Cloud Access Security Brokers

Fonte: Gartner Outubro/2020

7.5. Abaixo segue quadro comparativo conforme inciso II do art. 11, sendo feita verificação para composição da análise comparativa:

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1		X	
	Solução 2		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X

Quadro 01 - quadro comparativo de soluções conforme inciso II do art. 11

8. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

8.1. A solução 2, é considerada inviável para VALEC, pois os fabricantes não disponibilizam o CASB posicionado na infraestrutura local do cliente (on-premises), somente se por especificidade da regra de negócios do cliente, como exemplo, bancos e agências de segurança, que não podem ter informações de acesso a aplicações, assim como informações associadas aos usuários, ou outras informações que compõem a solução armazenadas na solução CASB posicionado na nuvem.

9. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

9.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 7.1 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

10. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

10.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 7.2 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

11. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

11.1. A Solução 1 de segurança do tipo CASB (SaaS) para proteção de dados e aplicações na nuvem contra ameaças Anti-Malware, vazamento de dados (DLP), e auditoria na nuvem. Broker (Proxy) posicionado na nuvem (SaaS) será a solução a ser contratada.

11.2. Sabe-se que na infraestrutura on-premises a figura de proteção do ativo Firewall, é voltado para proteção perimetral, mesmo sendo um Firewall Next-generation (NGFW) ou multicamadas este não possui características de inspeção na camada de serviços na nuvem, havendo uma lacuna de proteção, para o usuário que utiliza o serviço na nuvem.

11.3. Com a proteção de endpoints Antivírus Next-Gen no perímetro, tem-se o estabelecimento de uma camada para proteção anti-malware, para o dispositivo e para a rede corporativa, porém faz-se necessária a proteção da comunicação norte-sul, ao qual o software CASB é atuante tendo a missão de proteger os ativos da informação na nuvem contra vazamento de dados e infecções, com funcionalidade de auditoria integrada a solução.

11.4. A solução CASB propõe o preenchimento desta lacuna fazendo a proteção dos ativos e aplicações na nuvem, tendo como principais funcionalidades: controle contra vazamento de informações DLP, descobrimento de aplicações utilizadas pelos dispositivos, aplicação de segurança nos serviços da nuvem Office 365, GSuite, Box, AWS, proteção contra-malwares, visibilidade profunda das atividades do usuário/dispositivo através de detalhes granulares como identidade, dispositivo, tempo, localidade geográfica, atividades de auditoria, como criação, modificação, exclusão, compartilhamento, dentre outras.

11.5. Cabe ressaltar que as soluções tipo CASB quanto as features de DLP, buscam adequação junto a leis de proteção de dados GDPR, na Europa e LGPD no Brasil (lei 13709 de Ago/2018), incluindo templates para configurações de tratamento de dados, de informações sensíveis.

11.6. Assim, fica evidenciado neste ETP a necessidade de aquisição do software CASB, de forma estratégica e em consonância com a IN 01 de 2019 do SGD, que instrui a prevalência de contratação de soluções voltadas para a nuvem (SaaS). De acordo com a solução 1, o CASB ficará posicionado na nuvem do fornecedor/fabricante (SaaS), possuindo vantagens de alta disponibilidade, integridade e confiabilidade de acordo com o SLA de operação da solução, de 99,9%, item 4.61.

11.7. Ao se realizar o estudo deste ETP, observou-se que a solução de segurança CASB - Microsoft Cloud App Security (MCAS) em conjunto com outra solução a ser adquirida, conforme demonstrado no documento SEI 3715636 promove diversos fatores tecnicamente vantajosos tendo em vista a necessidade de economia de recursos.

11.8. Nota-se que outros fabricantes a partir do mapa comparativo na análise de custos, item 9 deste ETP, podem até ter um custo financeiro ligeiramente menor, entretanto há que se observar a vantajosidade oferecida pela solução de segurança CASB - Microsoft Cloud App Security (MCAS), onde através **da integração com a solução Microsoft Defender ATP** (Advanced Threat Protection) SEI 3715636, proporciona gestão mais efetiva, uma vez que trata logs, ações e detecções de comportamento de maneira centralizada, reduzindo riscos quanto a ácuracia e tempo de resposta na análise de uma ameaça ou aplicação não-sancionada. Dentre estas importantes integrações, 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 Antivírus 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. Mais especificamente, os domínios usados por esses aplicativos não-sancionados são propagados para dispositivos de endpoint para serem bloqueados pelo Microsoft Defender Antivírus dentro do SLA de proteção de rede.

VIII - Integração entre o serviço de identidade do Microsoft Azure AD (Azure AD Identity Protection);

IX - Dentre outras.

Fonte: https://docs.microsoft.com/en-us/cloud-app-security/mde-integration#investigate-devices-in-cloud-app-security [Acesso em 23/02/2021]

11.9. **Da integração da solução MS Cloud App Security necessárias 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 Cloud App Security;

VII - Rastrear atividades de usuário no Power-BI;

11.10. **Ainda, da integração da solução Cloud App Security 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 automaticamente 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;

Fontes: https://docs.microsoft.com/en-us/cloud-app-security/connect-office-365-to-microsoft-cloud-app-security [Acesso em 26/02/2021]

https://docs.microsoft.com/en-us/power-bi/admin/service-admin-auditing [Acesso em 26/02/2021]

https://docs.microsoft.com/en-us/cloud-app-security/protect-office-365 [Acesso em 26/02/2021]

12. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

12.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 7.3 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

13. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

13.1. Não se aplica tendo em vista tratar-se de um produto único.

14. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

14.1. Não se aplica.

15. PROVIDÊNCIAS A SEREM ADOTADAS ANTES DA CONTRATAÇÃO

15.1. Como o ambiente atual da Valec já possui o licenciamento da referida ferramenta, não há providências prévias a serem adotadas.

16. ANÁLISE DE CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

16.1. Conforme Termo de Referência SEI 3734548 , itens 5.6 e 8.

17. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS DE TRATAMENTO

17.1. Conforme Termo de Referência SEI 3734548 , itens 5.6 e 8.

18. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

18.1. Ao se identificar a utilização de dados da Valec alocados em nuvem e a tendência de aumento deste quantitativo, faz-se necessário a aquisição de software de segurança a fim de atender a proposta da infraestrutura nuvem (IaaS), através de cessão temporária de direito de uso (subscrição) usando a tecnologia da solução CASB contra ameaças provenientes de dispositivos corporativos (gerenciados) ou pessoais (não-gerenciados);

18.2. Nesse sentido, o planejamento em tela almeja os seguintes resultados:

- Economia no valor da aquisição;
- Eficiência com a redução do custo administrativo em função da redução da fragmentação de processos licitatórios;
- Efetividade com a padronização dos produtos e com a promoção de segurança mais profunda das informações;

- Eficácia com o atendimento das necessidades tecnológicas e de negócio da Valec.

18.3. A necessidade de proteção da camada norte-sul e consequente aplicação de auditoria, em vista da nova modalidade de acesso pelos usuários da VALEC aos serviços já alocados em nuvem como suíte de escritório MS Office 365, e-mail e futuros servidos *SaaS - (Software As A Service)* a serem contratados;

18.3.1. A utilização da solução CASB, através de software no formato de serviço na nuvem (SaaS), para atender a proteção ativa dos ativos da informação da VALEC contra ameaças de malwares provenientes de dispositivos corporativos (gerenciados) ou pessoais (não-gerenciados), proteção contra vazamento de dados (DLP), e disposição de uso de ferramenta de auditoria (em acordo com a PSI da VALEC, e em consonância com a LGPD) inclusa na solução para acessos com integração do serviço de gerência e identidade dos usuários da VALEC na nuvem, *Azure Active Directory*.

18.3.2. A solução provê, visibilidade de aplicações utilizadas nos dispositivos que conectam-se aos serviços da nuvem, contendo painéis(dashboards) das aplicações mais utilizadas, informações de dispositivos e usuários conectados, volume de tráfego, tempo de uso de cada aplicação na nuvem, e classificação do risco do uso, localização geográfica, auditoria de acessos, edição, cópia do arquivo e conteúdo, exclusão, download, upload.

18.4. Vantagens da utilização da solução:

I - Propiciar proteção aos ativos da informação e aplicações na nuvem para a regra de negócios da VALEC contra ameaças de malwares e vazamento de dados (DLP);

II - Propiciar mecanismo para Auditoria no acesso aos ativos da informação da VALEC dispostos na infraestrutura em nuvem (IaaS) como serviço (SaaS).

18.5. Considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente **VIÁVEL.**

19. APROVAÇÃO E ASSINATURA

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

19.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
_____ **CLÁUDIO AMORIM DE SOUSA** **Matrícula/SIAPE: 3218987**	_____ **ROBÉRIO XIMENES DE SABÓIA** **Matrícula/SIAPE: 1990222**

AUTORIDADE MÁXIMA DA ÁREA DE TIC (OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)
_____ **JORGE LUIS DA SILVA LUSTOSA** **Matrícula/SIAPE: 1105206**

Documento assinado eletronicamente por **Jorge Luis da Silva Lustosa**, **Superintendente**, em 01/03/2021, às 19:03, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Cláudio Amorim de Sousa**, **Gerente**, em 01/03/2021, às 19:06, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Sabóia**, **Integrante Requisitante**, em 01/03/2021, às 20:24, conforme horário oficial de Brasília, com fundamento no art. 3°, 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 **3715695** e o código CRC **28C32569**.

Referência: Processo nº 51402.100731/2020-14 SEI nº 3715695

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

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

Estudo Técnico Preliminar da Contratação/SUPTI-VALEC/DIRAF-VALEC-VALEC

Brasília, 29 de agosto de 2020.

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
26/01/2021	1.0	Finalização da primeira versão do documento	Luciane Inácia Lopes
11/02/2021	1.1	Revisão da primeira versão do documento	Cláudio Amorim de Sousa
26/02/2021	1.2	Revisão da segunda versão do documento	Robério Ximenes de Sabóia
27/02/2021	1.3	Revisão prévia de envio ao setor de licitações	Jorge Luis da Silva Lustosa

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO
INTRODUÇÃO

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1. INTRODUÇÃO

1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda SEI 3781122, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. Durante o Estudo Técnico Preliminar, diversos aspectos devem ser levantados para que os gestores certifiquem-se de que existe uma necessidade de negócio claramente definida, há condições de atendê-la, os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente.

1.3. O objeto do estudo é a **contratação de licenças de software do tipo Suíte de Escritório** que atendam de forma ampla às demandas da Valec Engenharia, Construções e Ferrovias S.A.

2. MOTIVAÇÃO/JUSTIFICATIVA

2.1. 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, dividido em estações de trabalho, notebooks, armazenamento híbrido, servidores, entre outros. A integração desses equipamentos e o software proporciona os meios que permitem o uso eficiente e eficaz desse conjunto tecnológico.

2.2. Com o fim da vigência do contrato de fornecimento de licenças Microsoft, faz-se necessária a manutenção das licenças Microsoft ou sua substituição por ferramenta equivalente que atenda aos requisitos e necessidades da Valec, considerando a necessidade de manter tal serviço de forma protegida e segura, atendendo a todos os normativos quanto a segurança de dados e informações.

2.3. 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).

2.4. 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 resolvam esses pontos.

2.5. Atualmente os empregados da Valec utilizam a solução Microsoft contendo Outlook, Word, Excel, PowerPoint, Publisher e Access com serviços Exchange, OneDrive, SharePoint, Planner e Teams.

2.6. A necessidade é que se mantenha toda essa solução ou que seja substituída por solução equivalente que preencha todos os requisitos necessários à Valec, considerando os itens abaixo:

a) Versões instaladas e sempre atualizadas;

b) Coautoria em tempo real para que vários usuários possam trabalhar simultaneamente no mesmo documento;

c) Cada usuário pode instalar os aplicativos de suíte de escritório em mais de um dispositivo;

d) Versões Web dos aplicativos Word, Excel e PowerPoint e Outlook ou equivalentes;

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

f) Hospedagem de e-mail com caixa de correio de 100GB.

2.7. Todas essas funcionalidades e ferramentas se encontram em plena utilização por meio da solução de suíte de escritório Microsoft Office 365 E3.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. **Identificação das necessidades de negócio**

3.1.1. Os requisitos de negócio são aqueles que independem de características tecnológicas e que definem as necessidades e os aspectos funcionais da Solução de Tecnologia da Informação.

3.1.2. As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição da solução mais adequadas a tais objetivos organizacionais, conforme relação a seguir:

3.1.2.1. Prover ferramenta para comunicação institucional por meio de troca de mensagens de correio eletrônico, com endereços/contas de e-mail pessoais e institucionais com alta disponibilidade e capacidade de armazenamento, chats de texto/imagens, inclusive com diálogos preservados de forma permanente para equipes

3.1.2.2. Disponibilizar ferramentas de apoio à automação de escritório para manter e possibilitar controles individuais de compromissos e tarefas, reuniões, controle de marcação de reuniões com compartilhamento da disponibilidade de agenda dos participantes, edição de textos e arquivos a serem publicados em intranet/internet, publicação compartilhada de arquivos em sítios de internet/intranet, edição de planilhas de cálculos matemáticos e manipulação de textos para tabulação e análise de dados e simulação de cenários e criação e manutenção de bancos de dados de pequeno porte.

3.1.2.3. Prover ferramentas para o planejamento e controle de trabalho em equipe, com compartilhamento de arquivos, chat permanente e gerenciamento de projetos colaborativos.

3.1.2.4. Permitir meios para gravação, manutenção e publicação interna de uma biblioteca de vídeos, bem como a geração de streaming para transmissão de eventos para público interno e externo.

3.1.2.5. Prover infraestrutura para armazenamento e compartilhamento de arquivos eletrônicos em ambiente de nuvem, com alta disponibilidade e segurança adequada nas condições de acesso, mesmo fora do ambiente de rede da Valec.

3.1.2.6. Disponibilizar todas as ferramentas de forma segura e remota quando necessário.

3.2. **Identificação das necessidades tecnológicas**

3.2.1. As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0) com adaptações, descrevem as características de uma solução que atende aos requisitos do negócio, detalhados após a realização de uma análise mais aprofundada. Dentre os requisitos da solução de tecnologia, são descritos:

3.2.1.1. Os requisitos funcionais, aqueles que descrevem capacidades que a solução será capaz de executar em termos de comportamentos e operações – ações ou respostas específicas de aplicativos ou componentes de tecnologia da informação,

3.2.1.2. Os requisitos não funcionais, aqueles que capturam condições que não se relacionam diretamente ao comportamento ou funcionalidade da solução, mas descrevem condições ambientais sob as quais a solução deve permanecer efetiva, ou qualidades que os sistemas precisam possuir. Também são conhecidos como requisitos de qualidade ou suplementares. Podem incluir requisitos relacionados à capacidade, velocidade, segurança, disponibilidade, arquitetura da informação e apresentação da interface com o usuário, e

3.2.1.3. Os requisitos de transição, aqueles que descrevem capacidades que a solução deve possuir com o objetivo de facilitar a transição do estado atual da organização para um estado futuro desejado, mas que não serão mais necessárias uma vez concluída a transição. São diferenciados dos outros tipos de requisitos porque são sempre temporários por natureza e porque não podem ser desenvolvidos até que ambas as soluções, a nova e a existente, sejam definidas.

3.2.2. Nesse sentido, a presente seção descreve os macro requisitos tecnológicos considerados para fins de identificação e definição da solução mais adequada, conforme relação a seguir:

3.2.2.1. Oferta de soluções de produtividade de escritório como edição de textos, planilhas e apresentações de forma colaborativa, com controles de versão.

3.2.2.2. Preferencialmente em modelo SaaS com vistas a possibilitar melhor controle do licenciamento dos produtos e por conseguinte melhor alocação dos recursos, além de manter o alinhamento à diretriz trazida pela alínea h do inciso II do artigo 11 da Instrução Normativa n° 01/2019 SGD/ME "*h) a possibilidade de aquisição na forma de bens ou contratação como serviço;*"

3.2.2.3. Permitir a atualização tecnológica;

3.2.2.4. Prever o suporte do fabricante;

3.2.2.5. Prever na solução de produtividade mecanismos de colaboração que permitam o trabalho de diferentes indivíduos simultaneamente em diferentes localidades;

3.2.2.6. Prever uma maior integração entre ferramentas, considerando o aumento da modalidade de teletrabalho;

3.2.2.7. Permitir proteção dos dispositivos utilizados no acesso à informação compartilhada;

3.2.2.8. Promover segurança das informações considerando a aplicação da Lei Geral de Proteção de dados - LGPD no que for aplicável;

3.2.2.9. Como requisitos funcionais, a solução deverá garantir:

a) Correio eletrônico

b) Mensagem instantânea e Webconference

c) Solução de videoconferência

d) Streaming de vídeo

e) Ferramenta de escritório e produtividade

f) Solução de arquivamento de mensagens de correio eletrônico

g) Integração de armazenamento seguro de dados com ambiente de produtividade

h) A solução possa ser unificada e que tenha compatibilidade com dispositivos móveis

3.2.2.10. A plataforma desses serviços devem ser acessadas independentemente do tipo de dispositivo utilizado pelo usuário, e de onde o usuário estiver, tendo em vista o crescente uso de dispositivos móveis e pessoais e o advento do teletrabalho. Deve-se também integrar múltiplas formas de comunicação e possuir ferramentas de escritório integradas que permita ganho de produtividade.

3.2.2.11. Por fim, deve ser considerado na solução a ser contratada, as necessidades corporativas acima citadas, as inovações tecnológicas, a situação orçamentária, a facilidade de implementar e operar, a gestão dos serviços e a segurança da informação.

3.3. **Demais requisitos necessários e suficientes à escolha da solução de TIC**

3.3.1. Além dos requisitos de negócio e tecnológicos, a presente seção destaca aqueles requisitos que devem ser considerados ao longo do planejamento da contratação para se assegurar o alcance aos objetivos pretendidos com a aquisição, conforme a seguir:

3.3.1.1. A solução deverá ser compatível com as demandas previstas no Plano Diretor de Tecnologia da Informação (PDTI) aprovado na Valec.

3.3.1.2. A solução deverá demonstrar a maior economicidade no aspecto financeiro e contratual, mantendo-se o nível técnico e tecnológico necessário, no mínimo, conforme descrito abaixo:

a) Ferramenta de Correio Eletrônico: Suporte a manutenção de contas de correio institucionais e contas de recursos, sem custos adicionais de licenciamento, além daqueles já aplicáveis aos usuários pessoais.

b) Sincronização com o ambiente Active Directory.

c) Ferramentas de gravação de vídeos e de reuniões de áudio/videoconferências: Suporte a gravação de vídeos das reuniões; Suporte a gravação e geração de streaming de eventos ao vivo.

d) Ferramentas de apoio à automação de escritório: Edição de textos em formato DOC, DOCX (Microsoft Word), RTF (Rich Text Format) e HTML; Edição de planilhas em formato XLX, XLXS (Microsoft Excel), CSV (texto separado por vírgulas) e HTML; Exportação/gravação de documentos/planilhas em formato PDF; Criação de macros em código de programação de alto nível para automação de tarefas repetitivas na ferramenta de automação de escritórios; Manutenção de bancos de dados em formatos ACCDB e MDB (Microsoft Access); Ambiente de ferramentas integradas entre si (edição de planilhas, textos, bancos de dados).

e) Ferramentas de segurança, compartilhamento e intercâmbio de arquivos: Criptografia forte de dados sensíveis; Controle de acesso e compartilhamento de arquivos que permita o intercâmbio e acesso aos recursos em ambiente de rede interna e mesmo em ambiente externo para os usuários do domínio de rede Valec.

f) Ferramentas de Chat em Grupo: chat de texto/imagens, inclusive com diálogos preservados de forma permanente para equipes.

g) Armazenamento e compartilhamento de arquivos na nuvem: Prover infraestrutura para armazenamento e compartilhamento de arquivos eletrônicos em ambiente de nuvem, com alta disponibilidade e segurança adequada nas condições de acesso, mesmo fora do ambiente da rede da Valec.

h) Compatibilidade com o S.O Windows 10: A solução deve ser compatível com o sistema operacional Windows 10, que é o atual SO do parque de computadores da Valec.

4. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

4.1. A presente sessão contém o registro do quantitativo estimado de itens para a composição da solução a ser contratada, de forma detalhada, e justificada, inclusive quanto à forma de cálculo. Busca-se descrever também os métodos, metodologias e técnicas de estimativas que foram utilizados, nos termos do inciso I do art. 11 da IN SGD-ME n. 01/2019.

4.2. A principal análise é referente a quantidade de servidores que irão utilizar as **ferramentas de escritório** no âmbito da VALEC através de estações de trabalho, notebooks, e de forma remota (teletrabalho) utilizando dispositivos móveis incluindo, notebooks, tablets, e smartphones.

4.3. Considerando a difusão e adesão do teletrabalho na empresa, o licenciamento Microsoft para suítes de escritório contempla o uso por usuário para até 15 (quinze) dispositivos: 5 (cinco) computadores, 5 (cinco) tablets, e 5 (cinco) smartphones.

4.4. Com o propósito de checar a quantidade de usuários ativos na VALEC foi realizada pesquisa na base de dados dos usuários da rede (serviço de diretório-autenticação).

4.5. Com o auxílio da ferramenta Power Bi, foram coletadas as informações necessárias para o quantitativo de usuários da rede conforme ilustra a imagem abaixo:

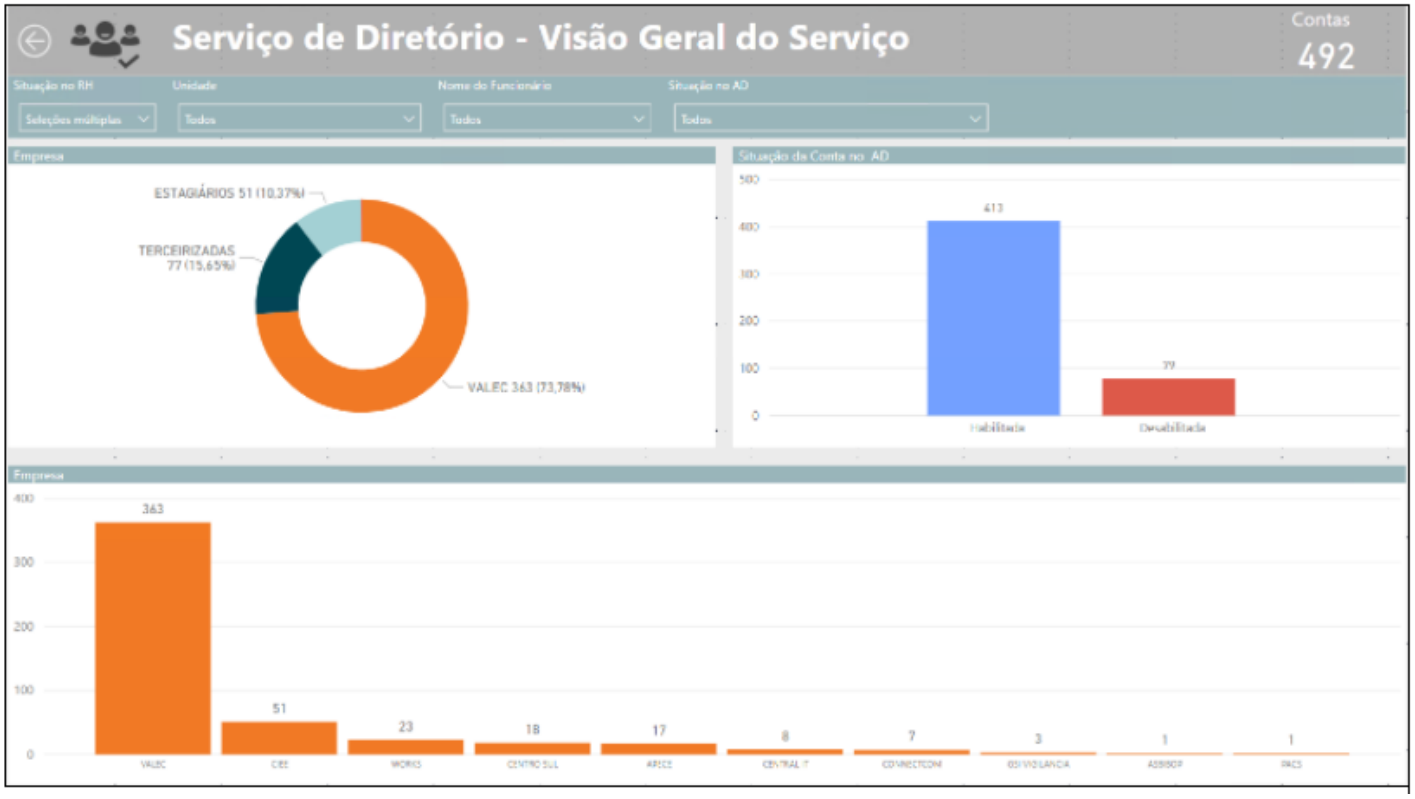


Fig. 01 - Painel de Usuários - Serviço de diretório - Visão Geral do Serviço (Extraído em 12/02/21) *Considerando o cenário atual com 79 contas desabilitadas.

4.6. No primeiro gráfico podemos observar que temos três tipos de usuários na empresa:

4.7. Usuários Valec: Compreendem servidores do quadro da VALEC, RFFSA, GEIPOT. Usuários que estão ativos, e não cedidos a outros órgãos. Estes usuários fazem uso dos computadores da empresa para execução diária de suas atividades laborais.

4.8. Usuários Estagiários: São estudantes de nível médio e superior. Cabe salientar que o contrato com o CIEE foi encerrado em dezembro último. Porém, na extração da informação do quantitativo, há época existiam 51 estagiários distribuídos nas 11 superintendências e 4 assessorias executando atividades administrativas de baixa complexidade e com prazo flexível para suas entregas, uma vez que são aprendizes. Há expectativa que seja celebrado novo contrato no primeiro semestre de 2021, atingindo o mesmo quantitativo.

4.9. Usuários Terceirizados: Compreende usuários de empresas com contratos ativos com a Valec, que prestam serviço em suas dependências, sejam elas obras ou dentro dos escritórios da Valec. Cabe esclarecer que a contratação desta solução não abrange a disponibilização de licenças ou computadores a empresas terceirizadas, uma vez que se tratam de recursos inerentes a prestação de serviço. Exceto em casos onde há previsão contratual de uso de recursos da contratante, como por exemplo os serviços de recepção, portaria ou suporte técnico, onde é desejável que a empresa use os mesmos recursos disponibilizados aos usuários com o propósito de compreender a perspectiva do usuário.

4.10. Nos gráficos subsequentes podemos observar como estes 3 grupos estão distribuídos na empresa. Cabe notar que neste painel o filtro utilizado foi da atual situação dos usuários e a empresa, excluindo usuários cedidos e terceirizados não habilitados ao uso do serviço. Por conta disto o total foi reduzido para 444 pessoas.

4.11. Da incorporação da EPL a Valec - Conforme matéria veiculada nos meios de comunicação conforme a publicação (3790025), onde o Ministério da Infraestrutura divulga o plano de incorporação da Empresa de Planejamento e Logística S.A. prevista para ocorrer no primeiro semestre de 2021. Cabe observar que foi celebrado o contrato de consultoria para estruturação do projeto, entre a Valec e a Empresa Falconi(51402.101308/2020-31), para estruturação técnica do projeto de incorporação. Até o momento ainda não foi possível estabelecer de maneira precisa o quantitativo final, logo foi considerado o quantitativo de funcionários efetivos daquela empresa, totalizando 121 pessoas, onde somando-se ao quadro de extração de dados da figura 01, têm-se o quantitativo final de 565 de usuários que serão cobertos pelas licenças a serem contratadas.

4.12. Baseado no estudo acima para atender a VALEC, estima-se a contratação dos seguintes itens, conforme tabela a seguir:

Nome do item	Quantidade
Suíte de Escritório composta por solução de produtividade e colaboração disponibilizada em ambiente na nuvem (SaaS) e para uso simultâneo em até 15 dispositivos.	565

5. ANÁLISE DO MERCADO FORNECEDOR

5.1. Nesta seção pretende-se apresentar os aspectos relacionados ao mercado fornecedor, apontando suas principais características e especificidades:

5.1.1. (I) identificação dos segmentos do mercado fornecedor que podem atender às necessidades da APF, evidenciando o entendimento sobre a segmentação dos fornecedores e seus respectivos modelos de fornecimento;

5.1.2. (II) apontar os principais fornecedores e atores de cada segmento, descrevendo a participação deles no mercado;

5.1.3. (III) identificar experiências dos potenciais fornecedores com órgãos públicos;

5.1.4. **Panorama atual de Soluções de Suíte de Escritório**

5.1.5. Segundo a consultoria independente G2 Crowd, as suítes de escritório são pacotes de software que contêm uma variedade de produtos focados na produtividade, como software de criação de documentos, software de planilhas e software de apresentação. Em alguns casos, outros programas, como o software de gerenciamento de projetos, estão incluídos no pacote. Esses pacotes podem ser oferecidos por meio de uma assinatura ou compra única. Muitas suítes também são de código aberto e de uso gratuito. Os pacotes de escritório são amplamente utilizados como software básico para empresas de qualquer tamanho. Eles podem ser usados para uma ampla gama de tarefas e geralmente são usados para melhorar a produtividade dentro de uma organização.

5.1.6. Os produtos que estão em uma trajetória de alto crescimento com base em índices de satisfação do usuário, crescimento de funcionários e presença digital, conforme gráfico apresentado pela G2 Crowd chamado de Momentum Grid Scoring, são: Office 365, reconhecido como líder atual, seguido pelo Office, G Suite e WPS.

Fig. 02 - Lideres Momentum

5.1.7. A seguir, são apresentadas algumas características atinentes aos modelos de comercialização dos produtos baseados em modelos de Software como Serviço (SaaS), observando as diretrizes da IN SGD-ME nº 01/2019.

5.1.8. **OFFICE 365**

5.1.8.1. O Office 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.

a) O plano Office 365 E1 destina-se a funcionários com perfil de uso que não necessita da versão desktop das aplicações office e do outlook, sendo possível trabalhar utilizando a versão web destes recursos. Este plano aplica-se a um perfil de uso básico.

b) O plano Office 365 E3 destina-se a funcionários com perfil de uso que requer mais recursos de email, segurança, comunicação por voz, aplicações de *Business Intelligence* e mecanismos de *compliance*.

c) O plano Office 365 E5 destina-se a organizações que já fazem uso intensivo de serviços de comunicação em nuvem, a exemplo da PABX em nuvem, uma vez que será possível a integração da aplicação com o sistema de telefonia virtual, bem como o aumento de segurança em toda a aplicação e a disponibilização do aplicativo Power BI.

d) 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).

5.1.8.2. Para melhor compreensão acerca do escopo de cada tipo de licença do produto office, apresenta-se a seguir um quadro comparativo disponibilizado pelo fabricante sobre a comparação das funcionalidades constantes de cada tipo de licença.

		Business	Business Essentials	Business Premium	ProPlus	F1	E1	E3	E5
	Estimated retail price per user per month $USD (with annual commitment)	$8.30	$5	$12.5	$12	$4	$8	$20	$35
Standard Services	Install Office on up to 5 PCs/Macs + 5 tablets + 5 smartphones per user	Business[1]		Business[1]	ProPlus			ProPlus	ProPlus
	OneDrive for Business – personal online document storage	1 TB	1 TB	1 TB	1 TB	2 GB[2]	1 TB	1-5+ TB[3]	1-5+ TB[3]
	Office mobile apps – Create/edit rights for commercial use of Office mobile apps[4]	●	●[5]	●	●	●[5]	●[5]	●	●
	Office for the web – Create/edit rights for online versions of core Office apps	●	●	●	●	●	●	●	●
	Microsoft Forms[17]	●	●	●	●	●	●	●	●
	Sway for Office 365[6]	●	●	●	●	●	●	●	●
	To-Do – Personal task management app		●	●		●	●	●	●
	PowerApps and Flow		●	●		●[7]	●	●	●
	Team collaboration & internal portals (SharePoint), Internal social networking (Yammer)		●	●		●[8]	●	●	●
	Email - 50 GB email, contacts, shared calendars (Exchange)		●	●		2 GB[9]	●	●[10]	●[10]
	Skype for Business, Microsoft Teams – Conferencing, meetings, IM/presence, chat-centered workspace		●	●		●[11]	●	●	●
	Shift scheduling, content sharing, and workgroup messaging			●		●	●	●	●
	Planner		●	●			●	●	●
	Microsoft Bookings			●				●	●
	Outlook Customer Manager, Invoicing, Business center, Listings, Connections & MileIQ			●[12]					
	MyAnalytics[13]		●	●			●	●	●
	Microsoft Stream					●[14]	●	●	●
Advanced Services	On-premises Active Directory synchronization for single sign on	●	●	●	●	●	●	●	●
	Mobile Device Management (MDM) for Office 365[15]	●	●	●	●	●	●	●	●
	Access to equivalent on-premise servers (Exchange, SharePoint, Skype for Business)						●	●	●
	Manual retention policies across workloads					●	●	●	●
	Legal compliance & archiving needs for email – archiving, eDiscovery, mailbox hold							●	●
	Information protection – message encryption, rights management, data loss prevention							●	●
	Enterprise Voice w/Skype for Business (on-prem only)[16]								●
	Office 365 Cloud App Security, Advanced Threat Protection Plan 2								●
	Office 365 Advanced Compliance (Advanced eDiscovery, Customer Lockbox, Advanced Data Governance, Service Encryption with Customer Key, Office 365 Privileged Access Management, DLP for Teams chat and channel conversations, Information Barriers, Advanced Message Encryption, Supervision)								●
	Data analytics and visualization (Power BI Pro)								●
	Phone System, Audio Conferencing								●

Fig. 03 - Quadro comparativo de Licenças. Fonte: Fabricante

5.1.9. **G-SUITE**

5.1.9.1. A solução G-Suite consiste em uma solução de colaboração e produtividade da Google também 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. O G-Suite reúne um conjunto de ferramentas de produtividade e colaboração do Google e as combina em um pacote para acesso entre as equipes. A lista de aplicativos inclui: Gmail, Hangouts, Calendário, Google+, Drive, Sites, juntamente com Google Docs, Planilhas, Formulários e Apresentações. Esta solução é ofertada em três categorias de planos: Basic, Business e Enterprise.

5.1.9.2. Para melhor entender os diferentes produtos relacionados à suite de escritório apresenta-se a seguir os diferentes planos apresentados pelo fabricante.

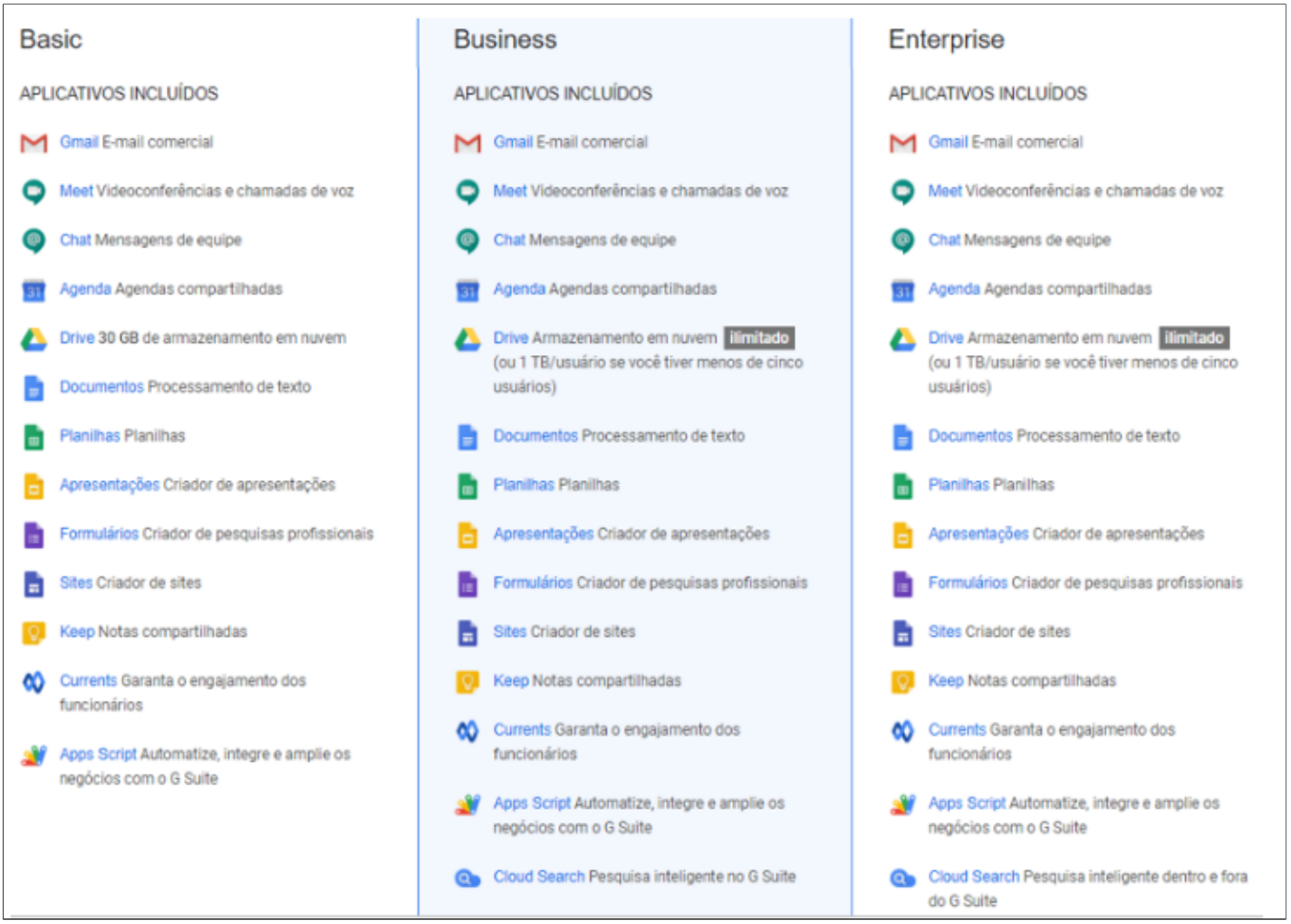


Fig. 04 - Quadro comparativo de Licenças. Fonte: Fabricante

5.1.10. **WPS**

5.1.10.1. A solução WPS consiste em uma solução de colaboração e produtividade da KINGSOFT também disponibilizada em ambiente de nuvem, que integra aplicativos essenciais na realização de atividades comuns relacionadas à produção digital de conteúdo e na organização dentro das equipes de trabalho.

5.1.10.2. Para melhor entender os diferentes produtos relacionados à suite de escritório apresenta-se a seguir os diferentes planos apresentados pelo fabricante.

WPS OFFICE Free	WPS OFFICE Premium	WPS OFFICE Professional
Completely Office suites	Completely Office suites	Completely Office suites
Read, Print and Save to PDF	Read, Print and Save to PDF	Read, Print and Save to PDF
WPS Special Paragraph Layout tool	WPS Special Paragraph Layout tool	WPS Special Paragraph Layout tool
5 pages PDF to Word	Convert PDF to Word	Convert PDF to Word
1G Cloud space	1G Cloud space	–
7 Days Version History	7 Days Version History	–
3 Devices (1 PC, 2 Mobile)	9 Devices (3 PCs, 6 Mobile)	1 PC
–	Removed Sponsored Access (no-AD)	Removed Sponsored Access (no-AD)
–	Split and Merge PDF to Word	Split and Merge PDF to Word
–	PDF Signature (only for Android)	–

Fig. 05 - Quadro comparativo de Licenças. Fonte: Fabricante

5.1.11. Já a consultoria independente TrustRadius apresentou uma visão da penetração dos produtos de suíte de escritório em usuários de diferentes escalas em função da quantidade de funcionários. Verifica-se nesse trabalho que o tamanho da empresa afeta a classificação da suíte de escritório que melhor atende as suas necessidades. Em estabelecimentos de pequeno porte (1 a 50 funcionários), as ferramentas G Suite, LibreOffice, Office 365 e Microsoft 365 foram as que melhor pontuaram. Em estabelecimentos de médio Porte (51 a 1000 funcionários), as ferramentas G Suite, OpenOffice, Libre Office, Office 365 e Microsoft 365 melhor pontuaram. Já em estabelecimentos de grande porte (mais de 1001 funcionários), as ferramentas que mais pontuaram foram a Microsoft Office 365, Office 365 e Microsoft 365 Business. O produto WPS não foi considerado por esse estudo.

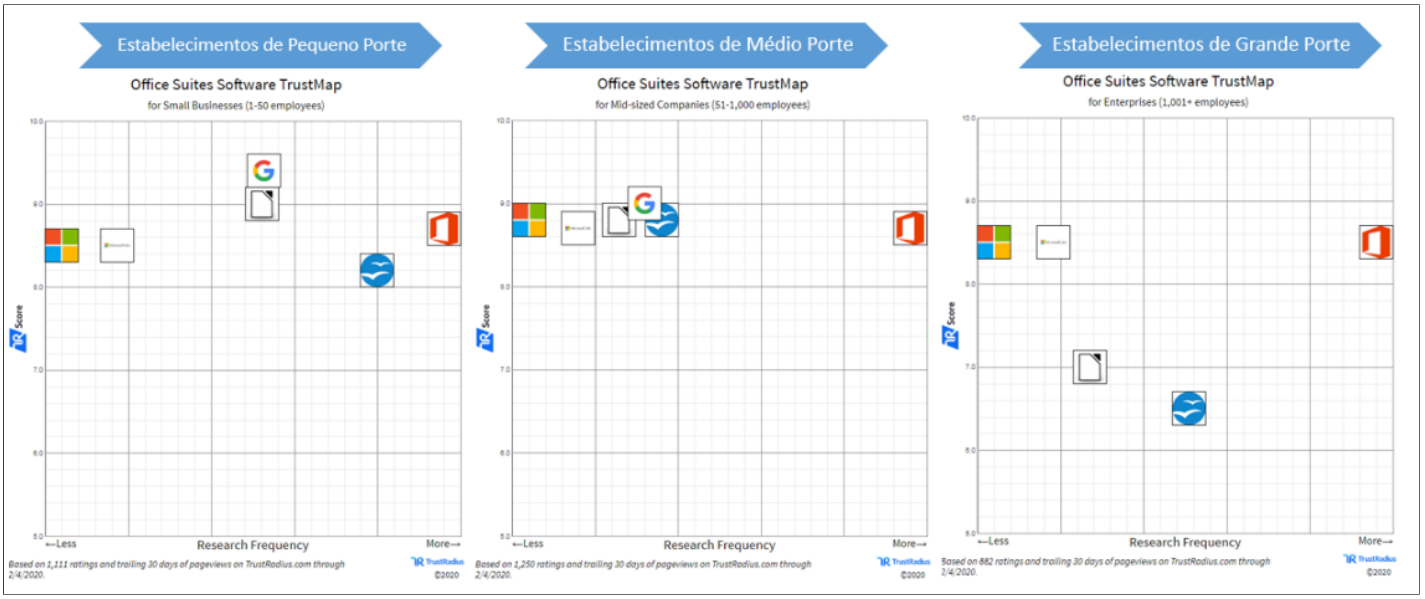


Fig. 06 - Visão de Penetração. Fonte: TrustRadius

5.1.12. Outro aspecto observado entre as soluções de suíte de escritório é a quantidade de clientes ativos nas plataformas. Nesse sentido, a consultoria independente Okta apresentou em seu relatório anual de análise de soluções de software de produtividade, ano 2020, uma evolução histórica da popularidade em termos de usuários ativos de diferentes ferramentas de

produtividade. Nesse estudo histórico, verifica-se que a solução Microsoft Office 365 mantém-se na liderança desde o início da série, apesar de a solução G Suite acompanhar o crescimento de usuários nos últimos anos.

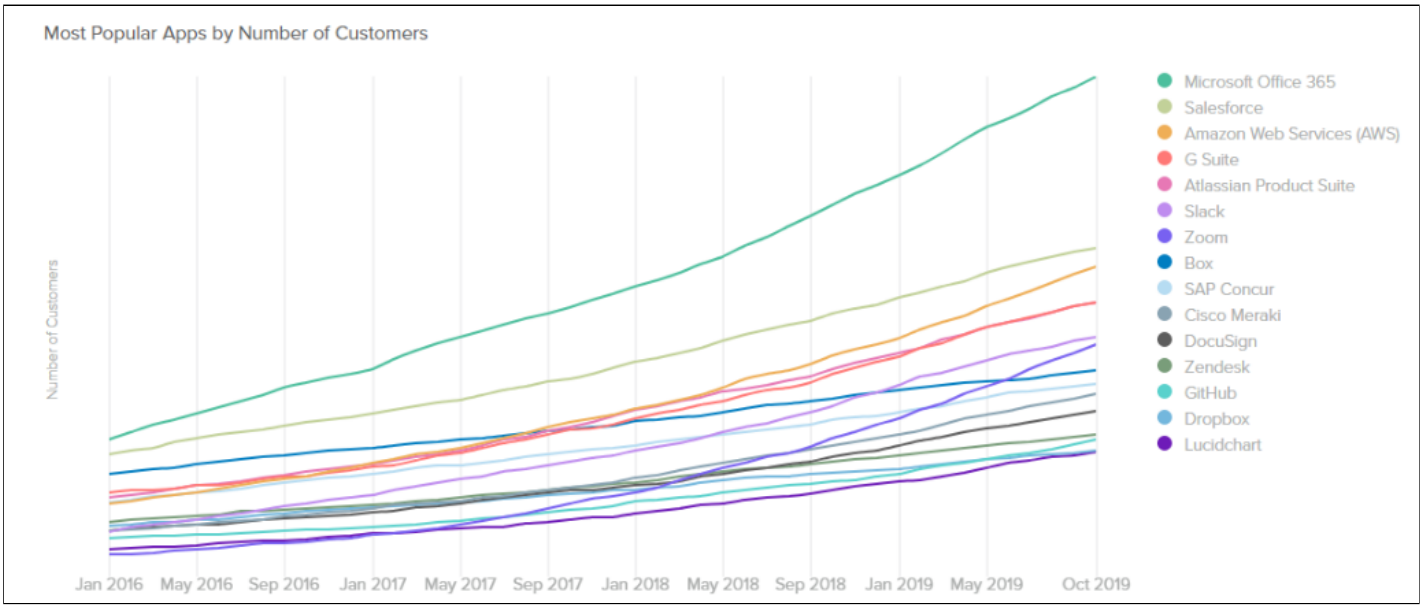


Fig. 07 - Evolução Histórica de Popularidade. Fonte: Okta

5.1.13. Após a apresentação de diferentes dimensões da atuação das ferramentas de suíte de escritório por meio de estudos de diferentes consultorias independentes, pode-se concluir que o mercado de soluções de softwares de produtividade é variado e que cada solução possui um segmento específico de atuação em termos do tamanho das organizações.

5.1.14. Outro aspecto a destacar diz respeito à previsão de consumo dos diversos produtos de suíte de escritório por empresas de diferentes portes. Nesse sentido, um estudo da consultoria independente Spiceworks mostra que o produto Microsoft Office 365 se destaca em termos de previsão de utilização, conforme gráfico a seguir.

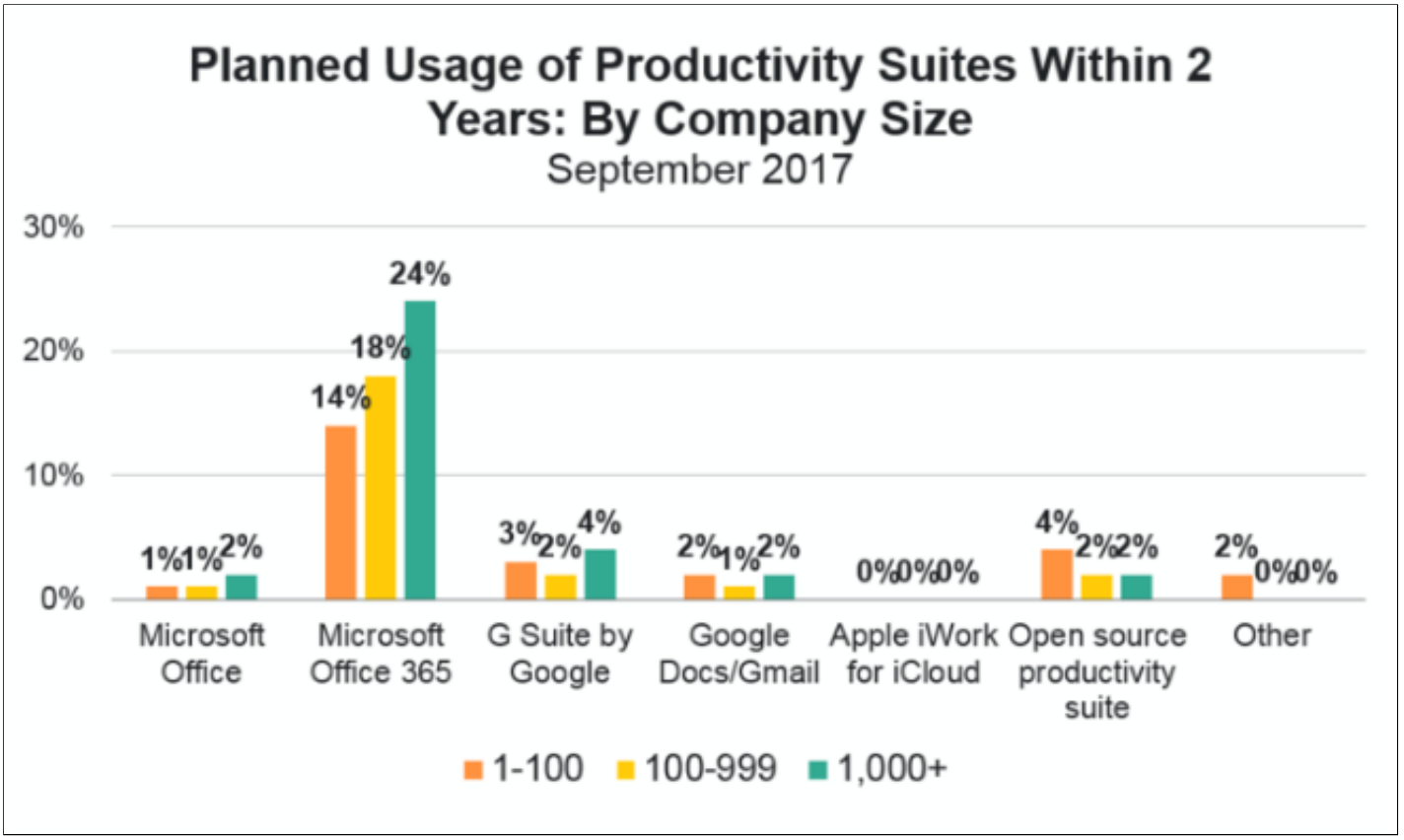


Fig. 08 - Produtividade. Fonte: SpiceWorks

6. ANÁLISE E IDENTIFICAÇÃO DE SOLUÇÕES DE MERCADO

6.1. Considerando o estudo de mercado anterior identificou-se as soluções a seguir que se apresentam como potenciais:

Id	Solução
1	Aquisição de Soluções G-SUITE
2	Aquisição de Soluções Office 365
3	Utilização de Soluções Livres combinadas com soluções pagas

6.1.1. **Solução 1 - Aquisição de Soluções G-SUITE na opção Business**

6.1.1.1. Descrição da solução: O G-Suite reúne um conjunto de ferramentas de produtividade e colaboração do Google e as combina em um pacote para acesso entre as equipes. A lista de aplicativos inclui: Gmail, Hangouts, Calendário, Google+, Drive, Sites, juntamente com Google Docs, Planilhas, Formulários e Apresentações.

6.1.1.2. Vantagens/Desvantagens da solução:

Vantagens	Desvantagens
- Solução de colaboração e produtividade também disponibilizada em ambiente de nuvem; - Reúne um conjunto de ferramentas de produtividade e colaboração que combina em um pacote para acesso entre as equipes.	- Impacto na migração e custos decorrentes.
- Aumento de competitividade	- Forma de proteção do sigilo de informações hoje já protegidas com as ferramentas atualmente disponíveis.
	- Treinamento da equipe técnica e dos próprios usuários;
	- Histórico de comunicações já existentes (frente às ferramentas hoje utilizadas): chats permanentes; arquivos compartilhados; acervo de vídeos de eventos armazenados (possíveis necessidades de conversão de formatos/protocolos/remanejamento de locais de armazenamento);

6.1.2. **Solução 2 - Aquisição de Soluções Microsoft 365**

6.1.2.1. Descrição da solução: Nesse cenário podemos fazer a manutenção do serviço Microsoft Office 365 com ferramentas disponíveis na modalidade de SaaS (software como serviço) da Microsoft. Os serviços incluem o acesso às diversas ferramentas online e também ao licenciamento do Microsoft Office em suas versões para instalação em desktop.

6.1.2.2. Vantagens/Desvantagens da solução:

Vantagens	Desvantagens
- Compatibilidade ampla entre os diversos aplicativos e serviços que compõem a solução, por serem do mesmo fabricante e serem comercializados em conjunto	- Concentração/dependência da solução técnica na oferta de um único fabricante, em detrimento de soluções parciais disponíveis no mercado que, em dado momento, podem ser superiores em cobertura de funcionalidades
- Forte grau de integração entre os serviços e aplicações	- Maiores riscos de problemas no processo de aquisição da solução (pregão eletrônico), pela concentração em um contrato de maior vulto financeiro.
- Grande cobertura de funcionalidades de automação de escritório e de trabalho em equipes	
- Oferta frequente de novas funcionalidades, melhorias e correções de bugs	
- Consistência da estrutura de suporte técnico à disposição para a solução	
- Ampla disponibilidade de treinamento para usuários e profissionais de TI no que concerne ao uso e suporte da solução	
- Expertise técnica e experiência da equipe de profissionais da Valec com a solução em questão, já estabelecidas, pois esta solução está em pleno uso no ambiente da Valec.	
- Comprovada continuidade da solução, pela solidez técnica e financeira da empresa que desenvolve a solução.	
- Todos os recursos materiais necessários para uso e para a infraestrutura da solução, como equipamentos, sistemas operacionais e infraestrutura de rede já estão disponíveis e dimensionadas adequadamente no ambiente da VALEC.	

6.1.3. **Solução 3 - Utilização de Soluções Livres associados com outros pagos.**

6.1.3.1. Descrição da Solução: Adoção de diversos softwares livres e pagos que cumpririam as funções hoje cobertas pela suíte Office 365 da Microsoft, sendo os principais, a suíte de aplicativos livre LibreOffice e o cliente de correio eletrônico Mozilla Thunderbird. Uma série de outros softwares e serviços seriam necessários para completar as funcionalidades atendidas pela suíte de escritório. Sem o compromisso de ser uma lista exaustiva, segue uma enumeração dos principais softwares e serviços necessários:

6.1.3.2. Fornecedores da solução (para implementar a solução 3 seria necessário associar diversos fornecedores):

a) Libre Office: The Document Foundation (organização sem fins lucrativos - sítio oficial: https://www.documentfoundation.org/);

b) Mozzila Thunderbird: Fundação Mozilla (organização sem fins lucrativos - sítio oficial: https://foundation.mozilla.org/pt/about/);

c) ExQuilla for Microsoft Exchange/Coruja: Beonex GmbH (sítio oficial: https://www.beonex.com/owl/);

d) Lightning (Calendário): Fundação Mozilla (organização sem fins lucrativos - sítio oficial: https://foundation.mozilla.org/pt/about/);

e) Trello: Atlassian (sítio oficial: https://www.atlassian.com/company);

f) Workplace: Facebook (sítio oficial: https://www.facebook.com/workplace/);

g) YouTube: Youtube (do grupo da Google – sítio oficial: http://www.youtube.com);

h) Amazon Drive: Amazon.com (sítio oficial: https://www.amazon.com.br);

i) Slack: Slack.com (sítio oficial: https://slack.com/intl/pt-br/about);

j) ToDoist: Doist (sítio oficial: https://doist.com/about-us/);

k) Evernote Business: Evernote Corporation (sítio oficial: https://evernote.com/intl/pt-br/about);

l) AxCrypt: AxCrypt AB (sítio oficial: https://www.axcrypt.net/about/);

m) Wix Premium Unlimited: Wix.com (sítio oficial: https://pt.wix.com/about/us).

6.1.3.3. Vantagens da solução como um todo:

Vantagens	Desvantagens
- A solução não está restrita a um só desenvolvedor, implicando em menor grau de dependência de desenvolvedores	- Riscos de continuidade das soluções parciais, por se tratarem de empresas, em sua maioria, novas no mercado, ainda sem a devida comprovação de solidez financeira
- Grande cobertura de funcionalidades de automação de escritório e de trabalho em equipes	- Eventual sombreamento de funcionalidades entre os serviços escolhidos
	- Baixo grau de padronização visual e modo de operação das soluções, por serem de múltiplos desenvolvedores
	- Apenas médio/baixo grau de integração entre as diversas soluções
	- Baixa padronização e consistência para se lidar com a estrutura de suporte técnico e treinamento dos usuários e técnicos de TI, por se tratarem de múltiplos desenvolvedores
	- Dificuldades técnicas e legais para contratação por meio de devido processo de licitação, porque uma boa parte dos fornecedores não possui representação comercial e/ou estrutura de suporte (a legislação de aquisições públicas não permite que uma empresa faça a venda e outra assuma as responsabilidades pelo suporte técnico, por meio de um único contrato público)
	- Maiores riscos de problemas no processo de aquisição da solução (pregão eletrônico), pela concentração em um contrato de maior vulto financeiro
	- Baixa expertise técnica e experiência da equipe de profissionais da Valec com a solução em questão.
	- Haveria grande necessidade de treinamento da equipe de usuários da Valec, bem como dos técnicos de TI, pois muitas mudanças na forma de usar e na infraestrutura de TI para suporte da solução seriam necessárias.

6.2. **Análise comparativa de soluções**

6.2.1. Examina-se nesta seção, para cada solução, os aspectos previstos na IN SGD-ME nº 01/2019 que devem ser avaliados em uma contratação de TIC.

Requisito	Solução	Sim	Não	Não se Aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1 - Aquisição de GSUITE	X		
	Solução 2 - Aquisição do Office 365	X		
	Solução 3 - Software livres	X		
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de Software)	Solução 1 - Aquisição de GSUITE		X	
	Solução 2 - Aquisição do Office 365		X	
	Solução 3 - Software livres	X (Alguns)		
A solução é composta por software livre ou software público? (quando se tratar de Software)	Solução 1 - Aquisição de GSUITE		X	
	Solução 2 - Aquisição do Office 365		X	
	Solução 3 - Software livres	X		
A solução é aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo ePing, eMag, e PWG?	Solução 1 - Aquisição de GSUITE			X
	Solução 2 - Aquisição do Office 365			X
	Solução 3 - Software livres			X
A solução é aderente às regulamentações da ICP- Brasil? (quando houver necessidade de certificação digital)	Solução 1 - Aquisição de GSUITE			X
	Solução 2 - Aquisição do Office 365			X
	Solução 3 - Software livres			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1 - Aquisição de GSUITE			X
	Solução 2 - Aquisição do Office 365			X
	Solução 3 - Software livres			X

7. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

7.1. Solução 3: Apesar da possibilidade de utilização de soluções gratuitas associadas a outros serviços pagos, os riscos associados na utilização de tais softwares, conforme citado nas desvantagens da solução 3, item 6.1.3.3, a falta de integração e padronização conforme exposto como necessidade tecnológica, no item 3.2 e, ainda, considerando a falta de suporte dos fabricantes, tendo em vista alguns softwares serem gratuitos, tornam essa solução inviável.

7.2. O iWork é a suíte de aplicativos corporativos da Apple e por ser exclusivo para os sistemas operacionais Mac OS e iOS que atualmente não é utilizado na Valec, uma vez que nosso parque utiliza Windows 10 nas estações de trabalho e notebooks. Logo, por conta desta limitação tecnológica, não fizemos a análise detalhada desta solução.

7.3. Por fim, não foi objeto dos presentes estudos a adoção do WPS office por conta da incompatibilidade entre as funcionalidades ofertadas por uma suíte de produtividade. A solução WPS office possui um rol de funcionalidades ainda mais restrito em relação às suítes da Google e da Microsoft.

8. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

8.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 3.1 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

9. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

9.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 3.2 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

10. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

10.1. Para que se atenda a demanda constante no item 4 deste ETPC, será contratada a solução Microsoft Office 365 nos quantitativos indicados no quadro a seguir:

Licença	Quantidade
Microsoft Office 365 E3	565
Core CAL Bridge for Office 365	565

10.2. Com a escolha dessa solução, se faz necessário a subscrição da licença Core CAL Bridge for Office 365 pois a mesma possibilita acesso do usuários aos serviços standard dos softwares Exchange Server, Skype for Business, System Center Configuration Manager, Windows Server e Sharepoint Server da Microsoft, que atualmente estão em uso na Valec.

10.3. No quadro abaixo está detalhado as características de cada Licença Office 365, sendo que a atualmente utilizada na Valec e que atende a sua necessidade é a Licença Office 365 E3, atendendo as necessidades de negócio e tecnológica, bem como a demanda demonstrada no item 4 deste ETPC.

Licenças	Descrição
Plano Office 365 E1	Serviços hospedados de colaboração e comunicação unificada, incluindo as seguintes funcionalidades: • Office Online – acesso aos aplicativos do Office no navegador para criação e edição de documentos; • Exchange Online Plano 1 – e-mail profissional com 50 GB de armazenamento na caixa de correio principal do usuário; • Skype for Business Online – reuniões online com áudio, vídeo HD e webconferência pela Internet. Mensagens instantâneas e transmissão de reuniões para até 10.000 pessoas; • Delve – central de conteúdo, pesquisa e descoberta, compilação de informações e análise de relacionamento com conteúdo, assuntos e contatos; • Planner – gerenciamento de trabalho. Planos de trabalho, organização e atribuição de tarefas, compartilhamento de arquivos e análise; • OneDrive for Business – armazenamento e compartilhamento de arquivos com, no mínimo, 1TB por usuário; • Sites de Equipe – compartilhamento de documentos com, no mínimo, 1TB de armazenamento de linha de base mais, no mínimo, 0,5GB por usuário; • Yammer – Rede social corporativa incluindo funcionalidades de colaboração e aplicativos de negócios do Yammer; • Sway – solução de narrativa digital incluindo relatórios, apresentações, boletins informativos e treinamentos; • Mobilidade – compatibilidade com Windows Phone, iOS e dispositivos Android; • Portal de vídeo empresarial;
Plano Office 365 E3	Serviços hospedados de colaboração e comunicação unificada, incluindo as seguintes funcionalidades: • Office 365 ProPlus – suíte de escritório contendo os aplicativos Word, PowerPoint, Excel, Outlook, One-Note, Publisher, Skype for Business e Access; • Office Online – acesso aos aplicativos do Office no navegador para criação e edição de documentos; • Exchange Online Plano 2 – e-mail profissional com 50 GB de armazenamento na caixa de correio principal do usuário e espaço ilimitado do Arquivo-Morto no Local;

	• Skype for Business Online – reuniões online com áudio, vídeo HD e webconferência pela Internet. Mensagens instantâneas e transmissão de reuniões para até 10.000 pessoas; • Delve – central de conteúdo, pesquisa e descoberta, compilação de informações e análise de relacionamento com conteúdo, assuntos e contatos; • Planner – gerenciamento de trabalho. Planos de trabalho, organização e atribuição de tarefas, compartilhamento de arquivos e análise; • OneDrive for Business – armazenamento e compartilhamento de arquivos com, no mínimo, 1TB por usuário; • Sites de Equipe – compartilhamento de documentos com, no mínimo, 1TB de armazenamento de linha de base mais, no mínimo, 0,5GB por usuário; • Yammer – Rede social corporativa incluindo funcionalidades de colaboração e aplicativos de negócios do Yammer; • Sway – solução de narrativa digital incluindo relatórios, apresentações, boletins informativos e treinamentos; • Mobilidade – compatibilidade com Windows Phone, iOS e dispositivos Android; • Portal de vídeo empresarial; • Gerenciamento dos aplicativos pela empresa;
Plano Office 365 E5	Serviços hospedados de colaboração e comunicação unificada, incluindo as seguintes funcionalidades: • Office 365 ProPlus – suíte de escritório contendo os aplicativos Word, PowerPoint, Excel, Outlook, One-Note, Publisher, Skype for Business e Access; • Office Online – acesso aos aplicativos do Office no navegador para criação e edição de documentos; • Exchange Online Plano 2 – e-mail profissional com 50 GB de armazenamento na caixa de correio principal do usuário e espaço ilimitado do Arquivo-Morto no Local; • Skype for Business Online – reuniões online com áudio, vídeo HD e webconferência pela Internet. Mensagens instantâneas e transmissão de reuniões para até 10.000 pessoas; • Delve – central de conteúdo, pesquisa e descoberta, compilação de informações e análise de relacionamento com conteúdo, assuntos e contatos; • Planner – gerenciamento de trabalho. Planos de trabalho, organização e atribuição de tarefas, compartilhamento de arquivos e análise; • OneDrive for Business – armazenamento e compartilhamento de arquivos com, no mínimo, 1TB por usuário; • Sites de Equipe – compartilhamento de documentos com, no mínimo, 1TB de armazenamento de linha de base mais, no mínimo, 0,5GB por usuário; • Yammer – Rede social corporativa incluindo funcionalidades de colaboração e aplicativos de negócios do Yammer; • Sway – solução de narrativa digital incluindo relatórios, apresentações, boletins informativos e treinamentos; • Mobilidade – compatibilidade com Windows Phone, iOS e dispositivos Android; • Portal de vídeo empresarial; • Ferramentas avançadas de conformidade; • Gerenciamento dos aplicativos pela empresa; • Proteção das informações (DLP); • Autoatendimento de Business Intelligence (BI) no Excel;

	• Cloud PBX; • PSTN Conferencing; • Power BI Pro – ferramentas de análise de negócios para analisar dados e compartilhar ideias. Data Discovery.
Core CAL Bridge for Office 365	Licença individual de usuários, complementar ao Office 365, aos serviços standard dos softwares Exchange Server, Skype for Business, System Center Configuration Manager, Windows Server e Sharepoint Server com Software Assurance.

11. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

11.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 3.3 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

12. JUSTIFICATIVAS PARA PARCELAMENTO OU NÃO DA SOLUÇÃO

12.1. Não se aplica tendo em vista tratar-se de um produto único.

13. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

13.1. Não se aplica.

14. PROVIDÊNCIAS A SEREM ADOTADAS ANTES DA CONTRATAÇÃO

14.1. Como o ambiente atual da Valec já possui o licenciamento da referida ferramenta, não há providências prévias a serem adotadas.

15. ANÁLISE DE CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

15.1. Conforme Termo de Referência SEI 3734548, itens 5.6 e 8.

16. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS DE TRATAMENTO

16.1. Conforme Termo de Referência SEI 3734548, itens 5.6 e 8.

17. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

17.1. A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

17.2. Nesse sentido, o planejamento em tela almeja os seguintes resultados:

- Economia no valor da aquisição;
- Eficiência com a redução do custo administrativo em função da permanência da mesma solução já utilizada na Valec;
- Efetividade com a padronização dos produtos e oferta de uma solução que objetiva maior produtividade e colaboração entre as equipes;
- Eficácia com o atendimento das necessidades tecnológicas e de negócio da Valec.

17.3. Observa-se ainda que conforme análise qualitativa e quantitativa sobre as diferentes soluções evidencia-se na Solução 2 - Aquisição de Office 365 E3, mostra-se vantajosa em termos econômicos conforme verificado na análise de custo total de propriedade entre diferentes soluções. O potencial de economia esperado abarca a dimensão unitária do valor gasto pela aquisição dos softwares de suíte de escritório, bem como a economia do custo de uma possível migração para outra solução.

17.4. A análise atende aos seguintes critérios direcionadores: redução dos custos totais para o atendimento de necessidades por bens e serviços, englobando eventuais despesas com contratos e demais gastos necessários ao atendimento das necessidades e oportunidades de padronização e integração de bens e serviços.

17.5. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis.

17.6. Considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente **VIÁVEL.**

18. APROVAÇÃO E ASSINATURA

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

18.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
_____ **JOSE AUGUSTO MEIRA DA ROCHA** **Matrícula/SIAPE: 2340257**	_____ **ROBÉRIO XIMENES DE SABÓIA** **Matrícula/SIAPE: 1990222**

AUTORIDADE MÁXIMA DA ÁREA DE TIC **(OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)**
_____ **JORGE LUIS DA SILVA LUSTOSA** **Matrícula/SIAPE: 1105206**

Documento assinado eletronicamente por **José Augusto Meira da Rocha**, **Integrante Técnico**, em 01/03/2021, às 15:55, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Sabóia**, **Integrante Requisitante**, em 01/03/2021, às 15:59, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Jorge Luis da Silva Lustosa**, **Superintendente**, em 01/03/2021, às 19:03, conforme horário oficial de Brasília, com fundamento no art. 3°, 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 **2743424** e o código CRC **2418C28B**.

Referência: Processo nº 51402.100731/2020-14 SEI nº 2743424

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

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

Estudo Técnico Preliminar da Contratação/GEINF-VALEC/SUPTI-VALEC/DIRAF-VALEC-VALEC

Brasília, 10 de fevereiro de 2021.

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
10/02/2021	1.0	Elaboração da primeira versão do documento	Luciane Inácia Lopes
27/02/2021	1.1	Revisão prévia de envio ao setor de licitações	Jorge Luis da Silva Lustosa

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Referência: IN SGD/ME nº 1/2019.

1. INTRODUÇÃO

1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda 3781122, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. Durante o Estudo Técnico Preliminar, diversos aspectos devem ser levantados para que os gestores certifiquem-se de que existe uma necessidade de negócio claramente definida, há condições de atendê-la, os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente.

1.3. O objeto do estudo é a contratação de **licenças Windows Server Datacenter e System Center** que atendam de forma ampla às demandas da Valec Engenharia, Construções e Ferrovias S.A.

2. MOTIVAÇÃO/JUSTIFICATIVA

2.1. A VALEC atualmente faz uso de 160 máquinas virtuais, sendo 48 com o sistema operacional Windows Server.

2.2. 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:

- Servidor AD, DNS, DHCP, TimeServer e NPS
- Nuvem Office 365 (Azure Connect)
- Power Bi Reporting Service
- Soluções de Controle de Acesso Fisico as instalações da empresa
- Assyst
- Varonis
- SQL Server
- Aplicativos de RH
- File Server
- Servidor de Orçamento de Obras Compor90
- E outros correlatos.

2.3. 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 necessário seu licenciamento.

2.4. O 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 de dispositivos de usuários, computadores e notebooks, que utilizam o Sistema Operacional Windows no ambiente da Valec.

2.5. De modo geral, a não renovação 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.

2.6. Resultados pretendidos:

2.6.1. Este estudo pretende demonstrar a viabilidade do licenciamento do sistema operacional Windows Server e System Center para a manutenção dos serviços e sistemas que estão alocados nos servidores Windows.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. **Identificação das necessidades de negócio**

3.1.1. Os requisitos de negócio são aqueles que independem de características tecnológicas e que definem as necessidades e os aspectos funcionais da Solução de Tecnologia da Informação.

3.1.2. As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição da solução mais adequadas a tais objetivos organizacionais, conforme relação a seguir:

3.1.2.1. Manter a licença atualizada de modo a garantir correções e a segurança de utilização do sistema.

3.1.2.2. Garantir o suporte do ambiente crítico de produção com suporte oficial do fabricante da solução 24 x 7.

3.2. **Identificação das necessidades tecnológicas**

3.2.1. As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0) com adaptações, descrevem as características de uma solução que atende aos requisitos do negócio, detalhados após a realização de uma análise mais aprofundada. Dentre os requisitos da solução de tecnologia, são descritos:

3.2.1.1. Os requisitos funcionais, aqueles que descrevem capacidades que a solução será capaz de executar em termos de comportamentos e operações – ações ou respostas específicas de aplicativos ou componentes de tecnologia da informação,

3.2.1.2. Os requisitos não funcionais, aqueles que capturam condições que não se relacionam diretamente ao comportamento ou funcionalidade da solução, mas descrevem condições ambientais sob as quais a solução deve permanecer efetiva, ou qualidades que os sistemas precisam possuir. Também são conhecidos como requisitos de qualidade ou suplementares. Podem incluir requisitos relacionados à capacidade, velocidade, segurança, disponibilidade, arquitetura da informação e apresentação da interface com o usuário, e

3.2.1.3. Os requisitos de transição, aqueles que descrevem capacidades que a solução deve possuir com o objetivo de facilitar a transição do estado atual da organização para um estado futuro desejado, mas que não serão mais necessárias uma vez concluída a transição. São diferenciados dos outros tipos de requisitos porque são sempre temporários por natureza e porque não podem ser desenvolvidos até que ambas as soluções, a nova e a existente, sejam definidas.

3.2.2. Nesse sentido, a presente seção descreve os macro requisitos tecnológicos considerados para fins de identificação e definição da solução mais adequada, conforme relação a seguir:

3.2.2.1. Compatibilidade com as seguintes tecnologias/soluções:

- Microsoft SQL Server
- Microsoft Sharepoint
- System Center Configuration Manager (SCCM)
- Compor90
- QUANTM
- Assyst

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

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

- 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. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

4.1. Para levantamento da quantidade necessária de licenças, considerou-se a quantidade de máquinas virtuais e a quantidade de máquinas físicas, considerando o número de núcleos/cores de seus processadores.

4.2. O datacenter da Valec concentra os principais serviços internos que suportam suas atividades finalísticas e seu ambiente é altamente virtualizado.

4.3. Neste ambiente há 48 máquinas virtuais Windows Server, desempenhando dentre outras, as seguintes funções:

- Serviços de Infra: AD, DHCP, DNS, RADIUS, ADRMS, ADFS
- Servidor de arquivos
- Bancos de dados SQL Server
- Reporting Services SQL

- SharePoint
- SCCM

4.4. Este ambiente virtualizado na plataforma Windows está hospedado em 2 servidores físicos em alta disponibilidade conforme quadro a seguir:

Modelo do servidor	Número de sockets	Número de cores por socket	Total de cores
PowerEdge R920	4	15	60
PowerEdge R920	4	15	60
		TOTAL	120

4.5. Conforme demonstrado, torna-se necessário o quantitativo de licenças suficientes para que se licencie o total de 120 cores.

5. ANÁLISE E IDENTIFICAÇÃO DE SOLUÇÕES DE MERCADO

5.1. Considerando a necessidade da demanda, identificou-se as soluções a seguir que se apresentam como potenciais:

Id	Solução
1	Manutenção do Windows Server e System Center
2	Contratação de outro Sistema Operacional com Suporte Empresarial
3	Adoção de Sistema Operacional livre

5.2. **Solução 1 -** Manutenção do Windows Server e System Center

5.2.1. Subscrição de licenças Microsoft Windows Server e System Center, com as seguintes características:

Vantagens	Desvantagens
- Manutenção dos serviços básicos de infraestrutura, eliminando necessidade de qualquer tipo de adequação, como migrações de Sistemas Operacionais e implantações de serviços em novas plataformas;	- Custo do licenciamento;
- Manutenção das aplicações existentes na Valec eliminando necessidade de quaisquer adequações/modificações nas mesmas;	- Diminuição da competitividade na licitação;
- Manutenção da compatibilidade com as soluções que utilizam unicamente plataforma Windows.	
- Manutenção das rotinas hoje executadas pelos usuários da Valec, sem necessidade de retrabalho e/ou mudança em qualquer tipo de processo existente;	
- Redução de custos com treinamentos básicos aos administradores de Sistemas Operacionais da Valec;	
- Suporte à solução garantido pelo fabricante.	

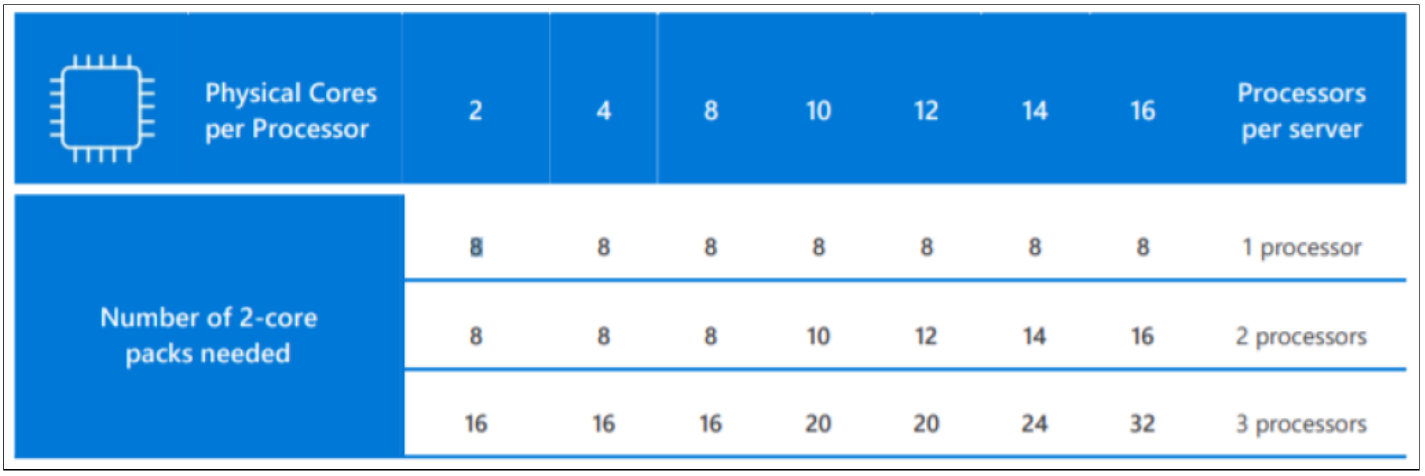
5.2.2. O Microsoft Windows Server é fornecido atualmente nas seguintes versões:

- Standard: indicado para ambientes físicos ou minimamente virtualizados.
- Datacenter: indicado para Datacenters e ambientes de nuvem altamente virtualizados.

5.2.3. Tanto o Windows Server Standard e quanto o Windows Server Datacenter são licenciados com base no número de núcleos (Cores) do processador da máquina física. Os requisitos para o licenciamento são:

- Todos os cores físicos devem ser licenciados
- Cada pacote de licenças cobre dois Núcleos (cores)
- Licenciar, no mínimo: 8 cores por socket e 16 cores por servidor.

5.2.4. A tabela abaixo, ilustra os requisitos descritos acima:



Physical Cores per Processor	2	4	8	10	12	14	16	Processors per server
Number of 2-core packs needed	8	8	8	8	8	8	8	1 processor
	8	8	8	10	12	14	16	2 processors
	16	16	16	20	20	24	32	3 processors

Fig. 01 - Requisitos para licenciamento. Fonte: Fabricante

5.2.5. O System Center garante o gerenciamento de todo o ambiente Windows do parque tecnológico.

5.3. **Solução 2 -** Contratação de outro Sistema Operacional com Suporte Empresarial

5.3.1. Contratação de Sistema Operacional de Servidor com Suporte Empresarial de outro fornecedor, diferente do atualmente utilizado na VALEC.

- Suse Linux Enterprise Server (https://www.suse.com/pt-br/products/server/)
- Red Hat Enterprise Linux (https://www.redhat.com/pt-br/technologies/linux-platforms/enterprise-linux)

5.4. **Solução 3**: Adoção de Sistema Operacional livre.

5.4.1. Substituição da utilização do Windows Server por Sistema Operacional de Servidor livre, que atenda às necessidades da VALEC.

5.4.2. Não foi encontrado Sistema Operacional de Servidor no Portal do Software Público Brasileiro (https://www.softwarepublico.gov.br/)./). Entretanto, existem diversos Sistema Operacionais de Servidor livres. Seguem algumas das ferramentas livres disponíveis na internet:

- CentOS (https://www.centos.org/)
- Ubuntu (https://ubuntu.com/)
- Debian (https://www.debian.org/index.pt.html)
- Fedora (https://getfedora.org/pt_BR/)
- FreeBSD (https://www.freebsd.org/)

5.5. Avaliação das soluções identificadas frente aos requisitos:

Requisitos	Solução 1 - Manutenção do Windows Server	Solução 2 - Contratação de outro Sistema Operacional com Suporte Empresarial	Solução 3 - Adoção de Sistema Operacional livre.
Suporte Oficial do Fabricante, 24 x 7	Atende	Atende	Não atende
Interoperabilidade/compatibilidade	Atende	Não atende	Não atende
Permitir pelo menos dois acessos simultâneos à Área de Trabalho Remota	Atende	Atende	Atende
Ser gerenciável a partir do SCCM	Atende	Atende parcialmente	Atende parcialmente

5.6. **Análise comparativa de soluções**

5.6.1. Examina-se nesta seção, para cada solução, os aspectos previstos na IN SGD-ME nº 01/2019 que devem ser avaliados em uma contratação de TIC.

Requisito	Solução	Sim	Não	Não se Aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	1	X		
	2	X		

	3	X		
A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de Software)	1		X	
	2		X	
	3		X	
A solução é composta por software livre ou software público? (quando se tratar de Software)	1		X	
	2		X	
	3	X		
A solução é aderente às políticas, premissas e especificações técnicas definidas pelos padrões de governo ePing, eMag, e PWG?	1			X
	2			X
	3			X
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			X
	2			X
	3			X
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	1			X
	2			X
	3			X

6. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

6.1. A Solução 2 e 3 se mostraram inviáveis por não terem atendido todos os requisitos necessários a manutenção das aplicações e sistemas da Valec conforme demonstrado no item 5.4.3 deste estudo.

7. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

7.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 5.1 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

8. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

8.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 5.2 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

9. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

9.1. Subscrição das licenças CIS Datacenter que inclui Windows Server e System Center em função do atendimento pleno aos requisitos de negócio, técnicos e funcionais especificados.

10. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

10.1. Tendo em vista o Orçamento Sigiloso, este item consta no item 5.3 do ANEXO ANÁLISE DE CUSTOS ESTUDOS TÉCNICOS PRELIMINARES SEI 3783843.

11. JUSTIFICATIVAS PARA PARCELAMENTO OU NÃO DA SOLUÇÃO

11.1. Não se aplica tendo em vista tratar-se de um produto único.

12. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

12.1. Não se aplica.

13. PROVIDÊNCIAS A SEREM ADOTADAS ANTES DA CONTRATAÇÃO

13.1. Como o ambiente atual da Valec já possui o licenciamento da referida ferramenta, não há providências prévias a serem adotadas.

14. ANÁLISE DE CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

14.1. Conforme Termo de Referência SEI 3734548, itens 5.6 e 8.

15. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS DE TRATAMENTO

15.1. Conforme Termo de Referência SEI 3734548, itens 5.6 e 8.

16. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

16.1. A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

16.2. Nesse sentido, o planejamento em tela almeja os seguintes resultados:

- Economia no valor da aquisição em função do ganho de escala com a contratação de Windows Server e System Center em conjunto por meio de um único produto;
- Eficiência com a redução do custo administrativo em função da redução da fragmentação de processos licitatórios;
- Efetividade com a padronização dos produtos;
- Eficácia com o atendimento das necessidades tecnológicas e de negócio da Valec.

16.3. Tendo em vista as maiores vantagens e o cumprimento dos requisitos essenciais para total atendimento da demanda, optou-se pela Solução 1, devendo ser contratadas 60 licenças do produto CIS Datacenter, que tem como descritivo o nome CoreInfrastructureSvrSteDCCore e SKU 9GS-00495, para atender os 120 cores dos dois servidores R920.

16.4. Tal solução atende ao critério de redução dos custos totais para o atendimento de necessidades por bens e serviços, e engloba eventuais despesas com contratos e demais gastos necessários ao atendimento das necessidades e oportunidades de padronização e integração de bens e serviços.

16.5. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis.

16.6. Considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente **VIÁVEL.**

17. APROVAÇÃO E ASSINATURA

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

17.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
_____ **JOSE AUGUSTO MEIRA DA ROCHA** **Matrícula/SIAPE: 2340257**	_____ **ROBÉRIO XIMENES DE SABÓIA** **Matrícula/SIAPE: 1990222**
AUTORIDADE MÁXIMA DA ÁREA DE TIC **(OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)**	
_____ **JORGE LUIS DA SILVA LUSTOSA** **Matrícula/SIAPE: 1105206**	

Documento assinado eletronicamente por **José Augusto Meira da Rocha**, **Analista de Sistemas**, em 01/03/2021, às 15:29, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Sabóia**, **Integrante Requisitante**, em 01/03/2021, às 15:59, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Jorge Luis da Silva Lustosa**, **Superintendente**, em 01/03/2021, às 19:07, conforme horário oficial de Brasília, com fundamento no art. 3°, 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 **3729013** e o código CRC **78DE7B11**.

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