INFRA S.A.
ASSEMBLEIA GERAL
CONSELHO DE ADMINISTRAÇÃO
DIRETORIA EXECUTIVA
DIRETORIA DE MERCADO E INOVAÇÃO
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

ANEXO I

Brasília, 15 de abril de 2024.

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

Tabela 1. *Lista de componentes da solução.*

Lote/Grupo	Item	SKU (Part Number)	Descrição	Nome do Produto	CATSER	Qtde.	Métrica	Modelo de Licenciamento	Qtde. Meses
1	1	9GS-00495	CIS Datacenter (Windows Server + System Center)	CISSteDCCore ALNG LicSAPk MVL 2Lic CoreLic	27502	60	Unidade	Subscrição	36
	2	7JQ-00341	SQL Server Enterprise com SA	SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic	27502	12	Unidade	Subscrição	36
	3	AAD-33204 + SYS-00001	Microsoft 365 E3 + Copilot Studio Legacy	M365 E3 Unified ShrdSvr ALNG SubsVL MVL PerUsr + Copilot Studio Legacy USL Sub Per User	27502	684	Unidade	Subscrição	36
	4	1NZ-00004	Defender For Endpoint Sever SubVL (Antivírus para Servidores)	Defender for Endpoint Server SubVL	27502	15	Unidade	Subscrição	36
	5	QLS-00003	Defender for Endpoint SubVL Per User (Antivírus para Usuários)	Defender for Endpoint SubVL Per User	27502	684	Unidade	Subscrição	36
	6	CE6-00004	Autenticação e gerenciamento de Endpoint (E5)	EntMobandSecE5Full ShrdSvr ALNG SU MVL EntMobandSecE3Full PerUsr	27502	684	Unidade	Subscrição	36
	7	NK4-00002	Power BI	Power-BI PRO	27502	111	Unidade	Subscrição	36
	8	7LS-00002	Microsoft Project	Project P3	27502	30	Unidade	Subscrição	36
	9	83I-00001	Copilot Modern Work	M365 Copilot Maneged Sub add-on	27502	72	Unidade	Subscrição	36

10	YFI-00001	Copilot Studio	Copilot Studio Sub Messages	27502	6	Unidade	Subscrição	36
11	1O4-00001	Power Automate	Power Automate Sub Per User	27502	43	Unidade	Subscrição	36
12	SEJ-00002	Power Apps	Power Apps Premium Sub Per User	27502	7	Unidade	Subscrição	36

1. **ITEM 1 - CIS DATACENTER (WINDOWS SERVER + SYSTEM CENTER)**

1.1. Compatibilidade com as seguintes tecnologias/soluções:

1.1.1. Microsoft SQL Server;

1.1.2. Microsoft Sharepoint;

1.1.3. System Center Configuration Manager (SCCM);

1.1.4. Compor90;

1.1.5. Assyst;

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

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

1.3.1. Gerenciamento de servidores e de estações de trabalho;

1.3.2. Inventário de software e de hardware;

1.3.3. Aplicação de patches de segurança;

1.3.4. Deploy de software;

1.3.5. Elaboração de relatórios;

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

2. **ITEM 2 - SQL SERVER ENTERPRISE COM SA**

2.1. Controle de redundância;

2.2. Controle de acesso aos dados;

2.3. Garantia de restrições de integridade

2.4. Controle de recuperação a falhas;

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

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

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

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

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

2.10. Estar em conformidade com a LGPD;

2.11. Poder rodar em Windows Servers e Linux;

2.12. Operar com dados estruturados e não estruturados;

2.13. Ter documentação sempre atualizada e disponível;

2.14. Permitir encriptação;

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

2.16. Permitir codificação UTF-8 de caracteres;

2.17. Permitir quantidade ilimitada de cores de CPU;

2.18. Permitir expansão ilimitada de memória;

2.19. Permitir virtualização de dados;

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

2.21. Permitir classificação de dados;

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

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

2.24. Permitir segurança a nível de registro;

2.25. Mascaramento de dados;

2.26. Particionamento de tabelas e índices.

3. **ITEM 3 -MICROSOFT 365 E3 + COPILOT STUDIO LEGACY**

3.1. A suíte deve possibilitar e incluir:

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

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

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

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

3.1.5. Publisher, e Access.

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

3.2.1. Word;

3.2.2. Excel;

3.2.3. PowerPoint;

3.2.4. Outlook;

3.2.5. OneNote;

3.2.6. Exchange;

3.2.7. OneDrive;

3.2.8. Skype for Business;

3.2.9. Microsoft Teams;

3.2.10. SharePoint;

3.2.11. Outlook;

3.2.12. Yammer;

3.2.13. Delve;

3.2.14. Stream;

3.2.15. Sway;

3.2.16. Power Apps;

3.2.17. Power Automate;

3.2.18. To Do.

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

3.3.1. Microsoft Intune;

3.3.2. Saúde do dispositivo para Analytics do Windows;

3.3.3. Microsoft 365 admin center;

3.3.4. Azure Active Directory Premium plan 1;

3.3.5. Informação de Proteção contendo:

3.3.5.1. Encriptação de mensagem;

3.3.5.2. Gerenciamento de acesso;

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

3.3.5.4. Windows Information Protection and Bitlocker;

3.3.5.5. Azure Information Protection;

3.3.6. Da capacidade de armazenamento:

3.3.6.1. Espaço de 5TB na nuvem por usuário.

3.4. Permite a automatização das tarefas rotineiras;

3.5. Minimizam os erros humanos, garantindo precisão das respostas;

3.6. Criação de tarefas e apresentações nas ferramentas de colaboratividade como o Power Point e Word;

3.7. Analisa dados e cria visualização integrados a ferramenta Excel;

3.8. Analisa códigos de desenvolvimento.

3.9. Sugere várias formas de redigir documentos.

4. **ITENS 4 E 5 - ANTIVÍRUS NEXT-GENERATION ANTI-MALWARE - (DEFENDER FOR ENDPOINT SERVER E USER)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.1.23.1. Dispositivos USB Drive (Pen Drive);

4.1.23.2. Dispositivos virtualizadores como VMWARE, VIRTUALBOX, através de USB Passthrough;

4.1.23.3. Dispositivos portáteis Windows.

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

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

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

4.1.24.1. Online — Com conexão com a Internet;

4.1.24.2. Offline — Sem conexão com a Internet.

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

4.1.25.1. Hijacking;

4.1.25.2. File Injection;

4.1.25.3. File Overflow;

4.1.25.4. In-Memory execution;

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

4.1.25.6. 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;

4.1.25.7. Escalation - LSASS Read e Zero Aliocate.

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

4.1.26.1. PowerShell;

4.1.26.2. Active Scripts — Jscript, WScript, CScript, rmacros, VBA.

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

4.1.27.1. Alertar;

4.1.27.2. Bloquear.

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

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

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

4.1.30.1. ZIP;

4.1.30.2. RAR;

4.1.30.3. GZIP;

4.1.30.4. TAR;

4.1.30.5. JAR;

4.1.30.6. WAR.

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

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

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

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

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

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

4.1.37. 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 Antivírus.

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2.13. Deve monitorar alterações em tarefas agendadas na máquina;

4.2.14. Deve monitorar tentativas de escalação de privilégios;

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

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

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

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

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

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

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

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

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

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

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

4.2.25.1. Tentativas de mascarar ou matar os processos no NGAV;

4.2.25.2. Detecção de Fileless Powershell malware;

4.2.25.3. Detecção da execução de comandos maliciosos em Powershell, como comandos que ocultam a execução do Powershell;

4.2.25.4. Invocação maliciosa de JavaScritps com Rundll;

4.2.25.5. Processos de Sistema Operacional iniciados por usuários que não são SYSTEM;

4.2.25.6. Executáveis iniciados do Recycle Bin;

4.2.25.7. Executável criado ou lançado como executável do Windows;

4.2.25.8. Processos do Windows sendo executados em pastas não padrão;

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

4.2.25.10. Uso do PSEXEC;

4.2.25.11. Modificação de host files;

4.2.25.12. Tentativa de invocação do Remote Shell;

4.2.25.13. Detecção de executável com múltiplas extensões;

4.2.25.14. Tarefas agendadas suspeitas;

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

4.2.26.1. Apagar arquivos;

4.2.26.2. Realizar Log Off de todos os usuários, ou usuários remotos, ou usuários interativos;

4.2.26.3. Suspender e terminar processos;

4.2.26.4. Gerar log de aplicação.

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

4.2.26.6. 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.

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

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

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

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

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

4.3.4.1. Log de Auditoria;

4.3.4.2. Dispositivos;

4.3.4.3. Proteção de Memória;

4.3.4.4. Script Control;

4.3.4.5. Ameaças;

4.3.4.6. Classificação de Ameaças;

4.3.4.7. Controle de Aplicação.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.3.19.1. instalação silenciosa;

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

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

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

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

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

4.3.25. O módulo de EDR deve ser gerenciado pela mesma console que o endpoint tradicional, não serão aceitas soluções que trabalham com mais de uma plataforma de gerenciamento.

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

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

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

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

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

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

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

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

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

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

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

4.3.36.1. Detalhar quais hosts de rede (estações, servidores) estão ativos, inativos ou desprotegidos, bem como detalhes deles;

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

4.3.36.3. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

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

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

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

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

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

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

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

4.3.41. O agente antivírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também

deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web;

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

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

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

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

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

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

4.3.48. Deverá possuir interface gráfica web, disponibilizada na língua portuguesa e inglesa, preferencialmente no idioma português;

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

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

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

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

4.3.52.1. Nome do dispositivo;

4.3.52.2. Início da proteção;

4.3.52.3. Último usuário logado no dispositivo;

4.3.52.4. Status do escaneamento em tempo real;

4.3.52.5. Último escaneamento realizado;

4.3.52.6. Status de proteção do dispositivo;

4.3.52.7. Grupo a qual o dispositivo faz parte.

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

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

4.3.55. Deve possibilitar instalação "silenciosa";

4.3.56. Deve permitir o bloqueio por nome de arquivo;

4.3.57. Deve permitir o rastreamento e bloqueio de infecções;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.3.75. Deve permitir a atualização automática dos agentes;

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

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

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

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

4.3.79.1. Nome da máquina;

4.3.79.2. Endereço IP;

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

4.3.79.4. MAC Address;

4.3.79.5. Usuário;

4.3.79.6. Versão do endpoint.

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

4.3.80.1. As 10 máquinas que mais receberam ocorrência de malware;

4.3.80.2. As 10 zonas que mais receberam ocorrência de malware;

4.3.80.3. Os 10 malwares que mais infectaram a rede;

4.3.80.4. Malwares por prioridade;

4.3.80.5. Malwares por classificação;

4.3.80.6. Históricos de infecções em estações/servidores;

4.3.80.7. Históricos de infecções em zonas.

4.3.81. Capacidade de exportar os indicadores para o formato CSV e PNG;

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

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

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

5. **ITEM 6 - AUTENTICAÇÃO E GERENCIAMENTO DE ENDPOINT (E5) - CLOUD ACCESS SECURITY BROKER (CASB)**

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

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

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

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

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

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

5.1.5.1. políticas pré-definidas;

5.1.5.2. customização de expressões regulares;

5.1.5.3. customização de dicionários;

5.1.5.4. prevenção de exportação de dados de contas corporativas para contas pessoais;

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

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

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

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

5.1.9. 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 INFRA S.A. e não-sancionados, conceito *Shadow IT;*

5.1.10. 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);

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

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

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

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

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

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

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

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

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

5.1.20. 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;

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

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

5.1.23. Deve ter habilidade de bloquear, redirecionar e alertar política violada possibilitando ou não o acesso, considerando a PSI da INFRA S.A.;

5.1.24. 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);

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

5.1.26. 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;

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

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

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

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

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

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

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

5.1.34. Identificar novas instâncias de aplicativos em nuvem dos provedores AWS, Google Cloud, Azure e outros, para aplicativos em nuvem adquiridos fora da TI da INFRA S.A.;

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

5.1.36. 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;

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

5.1.38. 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;

5.1.39. 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;

5.1.40. 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;

5.1.41. 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;

5.1.42. 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;

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

5.1.44. 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.;

5.1.45. 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;

5.1.46. 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;

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

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

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

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

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

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

5.1.53. 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;

5.1.54. 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;

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

5.1.56. 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;

5.1.57. 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;

5.1.58. Deve possuir Muti-Fator de Autenticação;

5.1.59. 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;

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

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

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

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

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

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

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

5.2.5. O CASB deve usar as informações de tráfego coletadas pelo agente de endpoint de Antivírus sobre os aplicativos e serviços em nuvem acessados a partir de dispositivos Windows 10 gerenciados pela TI. A integração

nativa permite que execução do Cloud Discovery em qualquer dispositivo da rede corporativa, usando Wi-Fi público, em roaming e por acesso remoto. Deve também permite a investigação baseada no dispositivo;

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

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

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

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

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

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

5.3.3. Colocar o usuário em quarentena;

5.3.4. Remover o colaborador específico;

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

6. **ITEM 7 - POWER BI PRO**

6.1. Criação de relatórios e painéis avançados;

6.2. Permitir a visualização e interação com conteúdo publicado no serviço Power BI;

6.3. Compartilhamento de relatórios;

6.4. Integração com ferramentas familiare;

6.5. Permita distribuição de relatórios elaborados para tomada de decisões.

7. **ITEM 8 - MICROSOFT PROJECT**

7.1. Relatórios personalizados: Possibilidade de criar relatórios customizados com tarefas, recursos, custos, entre outros;

7.2. Possibilidade de colaboração: A integração de ferramentas como o Teams ou Sharepoint nativo, permitem melhor comunicação facilitando o trabalho em equipe;

7.3. Acompanhamento do andamento de tarefas: Ter total controle sobre o andamento das tarefas do seu projeto;

7.4. Padronização das informações: Padronização e centralização das informações facilitando a gestão de seus projetos e programas;

7.5. Otimização do seu Portfólio: Possibilidade de avaliar e garantir melhores resultados de planejamentos com a gestão de tarefas e recursos, impulsionando o valor do seu portfólio;

7.6. Criação de modelos globais de cronograma: Possibilidade de criar modelos globais de cronograma para agilizar os seus planejamentos;

7.7. Controle de acesso e edição: Permitir controlar quem pode enviar ou mesmo acessar cronogramas, calendários, campos e outros recursos.

8. **ITEM 9 - COPILOT MODERN WORK**

8.1. Permite a automatização das tarefas rotineiras;

8.2. Minimizam os erros humanos, garantindo precisão das respostas;

8.3. Criação de tarefas e apresentações nas ferramentas de colaboratividade como o Power Point e Word;

8.4. Analisa dados e cria visualização integrados a ferramenta Excel;

8.5. Analisa códigos de desenvolvimento.

8.6. Sugere várias formas de redigir documentos.

9. **ITEM 10 - COPILOT STUDIO**

9.1. Permite a automatização das tarefas rotineiras;

9.2. Minimizam os erros humanos, garantindo precisão das respostas;

9.3. Criação de tarefas e apresentações nas ferramentas de colaboratividade como o Power Point e Word;

9.4. Analisa dados e cria visualização integrados a ferramenta Excel;

9.5. Analisa códigos de desenvolvimento.

9.6. Sugere várias formas de redigir documentos.

10. **ITEM 11 - POWER AUTOMATE**

10.1. Permitir a automação de processos e tarefas em sistemas, aplicativos de desktop e sites;

10.2. Criação de fluxos ilimitados para automação baseada em API;

10.3. Automatização de aplicativos legados com fluxos na área de trabalho;

10.4. Compartilhamento de relatórios;

10.5. Integração com ferramentas familiare;

10.6. Permita distribuição de relatórios elaborados para tomada de decisões.

11. **ITEM 12 - POWER APPS**

11.1. Permitir a criação de aplicativos personalizados de maneira fácil e rápida;

11.2. Compartilhamento de relatórios;

11.3. Integração com ferramentas familiare;

11.4. Permitir distribuição de relatórios elaborados para tomada de decisões.

Documento assinado eletronicamente por **MARCO ANTONIO GOÉS DE OLIVEIRA**, **Integrante Técnico**, em 17/04/2024, às 17:17, 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 Saboia**, **Integrante Requisitante**, em 18/04/2024, às 15:30, 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 **Renato Ricardo Alves**, **Superintendente de Tecnologia da Informação**, em 18/04/2024, às 17:00, 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 **Marcelo Vinaud Prado**, **Diretor de Mercado e Inovação**, em 19/04/2024, às 10:12, 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.transportes.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **8255723** e o código CRC **CBA7A340**.

SAUS, Quadra 01, Bloco 'G', Lotes 3 e 5. Bairro Asa Sul, - Bairro Asa Sul
Brasília/DF, CEP 70.070-010
Telefone: