ANEXO II

ESPECIFICAÇÕES TÉCNICAS

1. CARCTERÍSTICAS GERAIS

1.1. As Característica Gerais se aplicam à subscrição de 48 meses referente a virtualização de aplicações, conforme descrito, respectivamente, nos itens 2 e 3 deste Anexo;

1.2. Deverão estar inclusos na subscrição da solução toda parte de serviços de manutenção, suporte e atualização confirme descrito no item 4 deste Anexo;

1.3. A solução deve permitir e estar licenciada para o uso de aplicações virtuais em ambientes computacionais *On-Premises*, computação em nuvem privada, nuvem pública e em ambientes híbridos. A solução deve possibilitar a utilização desses ambientes de maneira simultânea, de modo que permita mover recursos entre esses ambientes;

1.4. A solução deverá estar licenciada para 20.000 usuários nomeados, e deve permitir que uma licença há mais de 30 dias sem uso possa ser reatribuída a um novo usuário;

1.5. O licenciamento deve ser exclusivamente por usuário, não devendo haver restrições quanto à quantidade de instalações que o Banco poderá fazer em seus ambientes. Ao licenciar os usuários, o Banco deverá poder instalar, por exemplo, toda a solução em um ambiente de Produção e em um ambiente de Homologação, ou em quantos ambiente mais se fizer necessário ao Banco;

1.6. Deverá suportar, no mínimo, os seguintes clientes de acesso, nas versões mais recentes e suportadas pelos fabricantes dos sistemas operacionais:

- Computadores com Sistema Operacional (SO) Microsoft Windows, Apple Mac e Linux, nas distribuições Red Hat, Ubuntu e derivados;
- Dispositivos móveis com SO Apple iOS e Google Android, incluindo Smartphones e Tablets;
- *Thin Clients* com SO baseado em distribuições Linux e Microsoft Windows;

1.7. Para entrega de aplicações publicadas, a solução deve permitir a integração de computadores servidores de aplicação em grupos (clusters) para sua criação a partir de uma imagem existente, entrega de serviço, modificação e gerenciamento;

1.8. Não deverão ser cotadas na proposta as licenças dos Sistemas Operacionais dos computadores servidores nos quais serão instalados os componentes de *software* da solução. O fornecimento dessas licenças será de responsabilidade da CONTRATANTE;

1.9. A solução deverá prover o licenciamento da plataforma de *hypervisor,* necessária ao seu funcionamento*,* mais otimizada para virtualização de aplicativos. Caso o *hypervisor* fornecido seja compatível com a solução de gestão de cloud provada do Banco (vCloud Suíte), este será integrado para facilitar a gestão e manutenção do ambiente;

1.9.1. A solução deverá prover alta disponibilidade através de instalação nos dois datacenters do BNB, usando o modo Ativo-Ativo;

1.10. Caberá à CONTRATADA a implementação da camada de virtualização, sendo de responsabilidade da CONTRATANTE a implementação de todo e qualquer *software* adjacente à solução conforme descrito no **Anexo III – Plano de Implantação**.

1.11. Permitir tráfego por meio de protocolo TCP e UDP simultaneamente, mediante políticas de acesso usando protocolo ICA, BLAST ou RDP;

1.12. Permitir a otimização de protocolo de comunicação, principalmente para ajustes em redes de baixa velocidade e/ou alta latência;

1.13. Permitir o sequenciamento da entrega dos dados na camada de transporte, inclusive durante falhas de rede temporária;

1.14. Permitir a combinação da forma de transporte (TCP e UDP) com base no *feedback* da experiência do usuário, durante a mesma sessão;

1.15. Permitir a correção e detecção de erros durante a transmissão da sessão estabelecida pelo usuário;

1.16. Quanto às tarefas de Operação e Monitoração, a solução deverá:

1.16.1. Possuir consoles Web de gerenciamento e controle com acesos baseados em RBAC;

1.16.2. Disponibilizar componente web que provenha visibilidade de sessões sobre TCP, apresentando dados em tempo real e dados históricos como latência *hop-by-hop* (L4), usuários, aplicações\desktops\ dispositivos;

1.16.3. Prover relatórios, seja para consumo de informações em tempo de execução ou como forma de agendamento, baseados em métricas como:

- Sessões ativas;
- Aplicações ativas;
- RTT, latência do protocolo, bandwidth, duração de sessão, duração de sessão, por pelo menos 60 dias.

1.16.4. Prover ferramenta Web que inclua, no mínimo, as seguintes funcionalidades:

1.16.4.1. Monitoramento de falhas em conexões classificadas por tipos, enumerando falhas, e disponibilizando dados de análise para cada uma dessas;

1.16.4.2. Monitoramento da infraestrutura do serviço, apresentada em camadas e integradas ao *Hypervisor;*

1.16.4.3. Monitoramento dos recursos, como CPU e memória de servidores apresentados em uma console web centralizada;

1.16.4.4. Monitoramento de falhas em aplicações publicadas virtualmente;

1.16.4.5. Monitoramento de sessões, possibilitando um *drilldown* em cada sessão de usuário com informações do *endpoint*, detalhes da sessão e canais do protocolo de comunicação acessíveis ao administrador, fornecendo visibilidade e uma lista completa de processos;

1.16.4.6. *Dashboard* gerencial com apresentação da infraestrutura, status de conexões e alertas que possam ser customizados e apresentados;

1.16.4.7. Políticas de alerta que possam ser definidas por métricas e alertas com possibilidade de envio de eventos via SNMP, ou através de e-mail nativo, e integração com soluções de monitoramento para fins de centralização de eventos de alertas;

1.16.4.8. Fornecer dados analíticos de tendência baseados em performance ou capacidade com período de retenção em 30 dias;

1.16.4.9. Fornecer visão sobre status do serviço de licenciamento e consumo de licenças no pool alocado;

1.16.4.10. Disponibilizar ações de controle sobre sessões de usuários que possibilitem aos administradores *logoff* de sessões, desconexão, envio de mensagem, espelhamento de sessões etc.;

1.16.4.11. Deverá fornecer mecanismos de testes sintéticos para aplicações publicadas, a fim de avaliar a disponibilidade de aplicações definidas como críticas;

1.16.4.12. Prover *insights* que possam sumarizar experiência de usuários com base em dados de duração de *logon*, falhas de sessões, etc.

1.17. Permitir a otimização em tempo real de áudio e vídeo para o Microsoft Teams, usando processamento específico para a solução ofertada.

1.18. A solução deverá garantir uma plataforma de acesso seguro aos aplicativos corporativos.

1.18.1. Catálogo recomendado e aplicações categorizadas conforme tutorial criado pelos administradores.

1.18.2. A solução deve permitir a experiência de customizar a plataforma com as cores e refletindo a identidade visual da companhia.

1.18.3. Permitir adicionar um endereço de site na plataforma para promoção ou divulgação de conteúdo corporativo, como intranet, portal web etc.

1.19. Plataforma de Acesso

1.19.1. Permitir funcionalidade de logon único (SSO) para aplicativos web e SaaS compatíveis com o protocolo SAML

1.20. Possuir acesso condicional permitindo o acesso ou não à aplicativos suportados baseados em políticas por aplicação como: dispositivo gerenciado ou não, versão de SO, faixa de rede.

1.21. Além do ambiente de produção, a solução também deverá permitir a criação de um ambiente de homologação, sem a necessidade de novo licenciamento.

1.22. Suportar a configuração de mecanismo de alta disponibilidade de forma nativa.

1.23. Permitir o escalonamento da solução de forma horizontal viabilizando a adição de novos servidores e o acréscimo de licenças de uso.

1.24. A infraestrutura para a instalação da solução será fornecida pelo CONTRATANTE, será a seguinte:

1.24.1.1. Microsoft Active Directory 2012 R2;

1.24.1.2. Windows Server 2012 R2 ou superior em plataforma 64 bits;

1.24.1.3. Sistema de Virtualização: VMware ESXi 6.0 Update 2 e VMware vCenter Server 6.0 U2 ou superior

1.24.1.4. Microsoft SQL Server Enterprise Edition, versão 2008 R2 ou superior, em instância compartilhada;

1.24.1.5. Cliente de conexão com banco de dados de 64 bits.

1.25. Permitir a criação de rotinas de backup agendadas, como também deve viabilizar a restauração da solução através da recuperação dela.

1.26. Suportar os seguintes protocolos e serviços de rede:

1.26.1.1. IPv4 e IPv6 (Internet Protocol);

1.26.1.2. DNS (Domain Name Services);

1.26.1.3. TCP (TransmissionControlProtocol);

1.26.1.4. UDP (UserDatagramProtocol)

1.26.1.5. Permitir a configuração e alteração de portas TCP/UDP que são utilizadas pelos componentes da solução.

2. SUBSCRIÇÃO DE VIRTUALIZAÇÃO DE APLICAÇÕES

2.1. Características da Solução:

2.1.1. Deverá permitir, na camada cliente, a publicação de aplicações para os seguintes navegadores de Internet: Microsoft Edge, Safari, Mozilla Firefox e Google Chrome;

2.1.2. Deverá permitir a publicação de qualquer aplicação, apresentada como método de Virtualização de Apresentação, no desktop cliente (camada cliente) desde que seja suportada pela solução de virtualização de aplicações quanto pela aplicação que será virtualizada;

2.1.3. A quantidade de licenças disponíveis deverá ser controlada, com emissão de alertas, ou por registro de ocorrência (log), sempre que seu número for insuficiente para atender à demanda;

2.1.4. Permitir administração centralizada dos computadores servidores que compõem a solução;

2.1.5. Permitir a configuração do método de autenticação de múltiplo fator (MFA), Além de suportar método de autenticação MFA de terceiros, deverá também incluir MFA nativo à solução, seja por meio de token, push ou e-mail;

2.1.6. Permitir que os servidores possam estar localizados fisicamente em locais distintos;

2.1.7. Possibilitar a criação de grupos de servidores (*farms*), para hospedagem da solução, com aplicações distribuídas entre diferentes servidores, sem a necessidade de softwares adicionais;

2.1.8. Possuir método de acesso otimizado para o mapeamento de drives visando priorizar o tráfego de dados, resultando na transferência de arquivos de ambos os lados de forma mais ágil;

2.1.9. Permitir a criação de políticas de utilização, baseadas em características do usuário, da rede ou dos servidores;

2.1.10. Permitir que o ambiente de administração possa ser executado remotamente e disponibilizado através de interface web;

2.1.11. Deve ter integração com o Microsoft Active Directory e Azure AD, possibilitando autenticar usuários e definir grupos de usuários e perfis de acesso;

2.1.12. Não possuir limitação da quantidade de aplicativos, usuários, grupos de usuários ou domínios exceto aquela definida pela quantidade de licenças;

2.1.13. Permitir o gerenciamento das licenças dos servidores de forma centralizada;

2.1.14. Permitir a configuração de regras de sessão por tempo de duração e por inatividade do usuário, para um autogerenciamento do uso do servidor;

2.1.15. A solução deve possuir tecnologia própria que permita a execução de várias sessões simultâneas, como por exemplo o Microsoft Remote Desktop Services;

2.1.16. Produtos que ampliam as tecnologias nativas da Microsoft na funcionalidade de Área de trabalho remota serão aceitos, desde que devidamente licenciados junto ao fabricante;

2.1.17. Suporte à criação de aplicações virtuais legadas, usando solução de empacotamento nativo da solução de virtualização. Permitir a integração com as aplicações Microsoft App-V;

2.1.18. Suporte a Unidade de Processamento Gráfico (*Graphics Processing Unit* - GPU) no servidor de aplicações;

2.2. Recursos de acesso e integração do usuário com as aplicações:

2.2.1. Deve possuir SSO (*Single Sign- On*) na execução das aplicações integrado com a autenticação local do desktop na rede corporativa e com a autenticação do portal WEB da solução para usuários externos;

2.2.2. Permitir o acesso aos aplicativos por meio de conexões de baixa velocidade ou alta latência;

2.2.3. Permitir que a interface de acesso web seja customizada e adaptada para os padrões e necessidades da contratante;

2.2.4. Permitir compartilhamento de sessão para que administradores do ambiente possam interagir com a sessão do usuário;

2.2.5. Permitir aos usuários o controle do aplicativo no que se referir às configurações de: áudio, tamanho de janela e resolução da tela;

2.2.6. Permitir que o usuário possa continuar o seu trabalho, exatamente no ponto onde parou, caso ele precise mudar de estação de trabalho ou reativar a sessão interrompida por queda de conexão, ou ainda, abrir a sessão em um outro tipo de equipamento. Essa característica deverá fechar a sessão do usuário aberta no dispositivo inicial e abri-la no novo dispositivo, permitindo que a aplicação “siga” o usuário;

2.2.7. Deve permitir que usuários de desktop Win32/64 e Linux possam alternar entre aplicativos locais e aplicativos remotos com ALT+TAB ou com a barra de tarefas do desktop local;

2.2.8. Deverá permitir o mapeamento automático de drives, portas paralelas, portas seriais e USB locais;

2.2.9. Deverá permitir detecção e criação automática de impressoras para os usuários e disponibilização de driver universal de impressão, de forma a não exigir a instalação de drivers específicos para cada tipo de impressora local no cliente;

2.2.10. A solução deverá implementar suporte a marca d'água nativa na solução, para fins de segurança da informação;

2.2.11. A solução deverá implementar gravação de sessão de Aplicações para fins de auditoria, suporte e outros;

2.3. Recursos de Segurança:

2.3.1. Deverá possuir criptografia de 128 bits ou superior entre cliente e servidor, de forma nativa, sem a necessidade de softwares adicionais;

2.3.2. Deverá possuir proteção contra key-logging (Keylogging é a ação de gravar/registrar as teclas pressionadas em um teclado).

2.4. Balanceamento de Carga:

2.4.1. Deverá permitir o balanceamento de carga entre os computadores servidores de aplicações da solução implementando no mínimo as seguintes características:

2.4.1.1. Permitir a monitoração de carga dos servidores em tempo real;

2.4.1.2. Para efeito de balanceamento de carga inteligente entre servidores de serviços de acesso a aplicações remotas o *software* deverá identificar e estabelecer a conexão do usuário com o servidor menos carregado, levando em conta fatores como uso de CPU, uso de memória e do número de sessões em execução;

2.4.1.3. Não deverá ser necessária a instalação de softwares adicionais nas estações para o funcionamento do balanceamento de carga.

3. GESTÃO DE DISPOSITIVOS

3.1. Características da Solução:

3.2. A solução precisa garantir uma plataforma de acesso seguro aos aplicativos corporativos.

3.3. Permitir que os colaboradores estejam conectados e produtivos a partir de qualquer lugar e com qualquer dispositivo com a solução multiplataforma de acesso digital.

3.4. Permitir personalizar a aplicação usada com serviços adicionais, tais como:

3.4.1.1. Permitir que os funcionários possam acessar, instalar e visualizar aplicações de forma nativa, aplicações móveis, SaaS e aplicações virtuais com single *sign-on* (SSO), juntamente ao catálogo de serviço.

3.5. Catálogo recomendado e aplicações categorizadas conforme tutorial criado pelos administradores.

3.6. Permitir aos funcionários pesquisarem colegas de trabalho, cargo, telefone de contato, visualizar organograma, iniciar uma chamada telefônica ou o envio de e-mails.

3.7. Possuir ferramenta que envolva e comunique os dispositivos gerenciados para uma melhor comunicação informativa ou acionável.

3.8. Permitir aos funcionários a habilidade de acessar portal de perguntas e respostas em um portal de autosserviço, artigos de base de conhecimento, telefone e e-mail de contato para suporte.

3.9. A solução deve permitir a experiência de customizar a plataforma com as cores e refletindo a identidade visual da companhia.

3.10. Permitir adicionar um endereço de site na plataforma para promoção ou divulgação de conteúdo corporativo, como intranet, portal web etc.

3.11. Permitir uma experiência aos funcionários contratados por meio da plataforma de acesso em um navegador e prover acesso aos recursos selecionados antes do início efetivo de suas atividades.

3.12. Permitir funcionalidade de logon único (SSO) para aplicativos web e SaaS compatíveis com o protocolo SAML

3.13. Acesso condicional permitindo o acesso ou não à aplicativos suportados baseados em políticas por aplicação como: dispositivo gerenciado ou não, versão de SO, presença de Jail Broken, faixa de rede e tempo de sessão

3.14. Suporte a multi fator de autenticação (MFA) compatíveis com Radius

3.15. Portal único para aplicações SaaS, Móveis Públicas, internas com opção de versionamento, Windows, Virtuais VMware e Citrix.

3.16. Permitir integração com outras ferramentas de Identidade, incluindo Active Directory, Azure Active Directory, LDAP, Okta, Ping etc.

3.17. Permitir o gerenciamento de dispositivos móveis e aplicações.

3.18. Permitir aplicação de configurações de segurança nos dispositivos móveis.

3.19. Permitir associação de mais de um dispositivo móvel a um mesmo usuário.

3.20. Possuir componente que viabilize o gerenciamento seguro dos dispositivos móveis que estejam logicamente localizados na rede interna do CONTRATANTE.

3.21. Possuir componente ou porção instalável que viabilize o gerenciamento seguro dos dispositivos móveis que estejam logicamente localizados fora da rede interna do CONTRATANTE.

3.22. Permitir que seja configurado o termo de aceite de uso do dispositivo móvel e permitir configurar a obrigatoriedade da aceitação do termo de aceite de uso do dispositivo móvel pelos usuários.

3.22.1.1. O texto do termo de aceite de uso do dispositivo móvel deve ser configurável pelas equipes do CONTRATANTE.

3.23. A solução deve registrar a informação de qual usuário realizou o aceite dos termos de uso e a data e hora;

3.24. A solução deve possuir mecanismos para buscar e exibir os eventos de aceite dos termos de uso realizados pelos usuários.

3.25. Permitir criação de loja corporativa (Enterprise AppStore) que possibilite que os usuários dos dispositivos móveis gerenciados instalem os aplicativos disponíveis na loja.

3.26. Permitir criação de container seguro/sandbox (funcionalidade que isola no dispositivo móvel gerenciado o acesso aos dados e aplicativos corporativos do acesso aos dados e aplicativos pessoais).

3.27. Suportar múltiplos usuários por dispositivo móvel, ou seja, permitir autoconfiguração do dispositivo baseando-se no usuário que está autenticado.

3.28. Permitir a configuração de, no mínimo, 2 (dois) perfis de e-mail.

3.29. Estes perfis devem permitir a configuração de maneira concorrente e devem ser compatíveis com o cliente nativo de e-mail utilizado no dispositivo móvel gerenciado ou com o aplicativo de e- mail seguro fornecido pelo fabricante da solução de gerenciamento.

3.30. Os perfis de e-mail devem suportar, no mínimo, as seguintes configurações:

3.30.1.1. E-mails com o mesmo domínio;

3.30.1.2. E-mails com domínios diferentes.

3.31. A solução contratada deve ser capaz de identificar e gerenciar, as seguintes características no dispositivo móvel:

3.31.1.1. Nome do dispositivo móvel;

3.31.1.2. Marca do dispositivo móvel;

3.31.1.3. Modelo do dispositivo móvel;

3.31.1.4. Sistema operacional e versão instalado no dispositivo móvel;

3.31.1.5. Integridade do sistema operacional instalado no dispositivo móvel;

3.31.1.6. Sistema operacional adulterado por técnicas de acesso privilegiado como root e *jailbreak*;

3.31.1.7. Identificador exclusivo do equipamento (UDID, INID, PIN, ICCID(s), IMEI(s), IMSI, MEID, Device ID, dentre outros);

3.31.1.8. Endereço MAC da interface Wi-Fi;

3.31.1.9. Endereço MAC da interface *bluetooth*;

3.31.1.10. Tipo de rede em uso (GSM, EDGE, GPRS, WCDMA);

3.31.1.11. Informação de estado da internet móvel (ativa ou inativa);

3.31.1.12. Conexões Wi-Fi e VPN configuradas;

3.31.1.13. Perfis instalados pela solução de gerenciamento.

3.32. Permitir a instalação, a atualização e a remoção de aplicativos.

3.33. Permitir o bloqueio da execução de aplicativos.

3.34. Permitir a configuração remota de aplicativos.

3.35. Permitir o bloqueio da instalação e a aquisição de aplicativos online.

3.36. Permitir a configuração e emissão de alertas para o administrador quando da violação de uma ou mais políticas configuradas.

3.37. Permitir o bloqueio do uso de mídias de armazenamento externo no dispositivo móvel.

3.38. Permitir desabilitar a câmera do dispositivo móvel.

3.39. Permitir o bloqueio do uso das funcionalidades de hotspot Wi-Fi e uso do bluetooth do dispositivo móvel.

3.40. Permitir a exclusão remota dos dados corporativos (wipe seletivo) armazenados no dispositivo móvel.

3.41. Permitir a exclusão remota dos dados corporativos (wipe seletivo) armazenados no dispositivo móvel quando detectada adulteração da integridade do sistema operacional.XXVIII. Permitir a redefinição remota das configurações do dispositivo móvel para o padrão de fábrica (factory default reset), bem como, permitir a exclusão dos dados das memórias internas e externas do dispositivo (wipe completo).

3.42. Possuir, no mínimo, o gerenciamento dos seguintes aplicativos, para utilização nos dispositivos móveis:

3.42.1.1. Navegador web com suporte ao acesso de páginas internas via vpn por aplicação

3.42.1.2. Leitor de documentos que suporte, no mínimo, as extensões .xls, .xlsx, .doc, .pdf, .ppt e .pptx.

3.42.1.3. Aplicativo de e-mail compatível com Exchange, Office 365, IBM Notes

3.43. Permitir que os aplicativos gerenciados suportem a configuração de servidor proxy quando o aplicativo necessitar de acesso à internet.

3.44.Permitir a instalação remota de aplicativos para um usuário ou para um grupo de usuários;

3.45. Permitir a criação de grupo de aplicativos baseado em perfil do usuário.

3.46. Permitir a atualização automática dos aplicativos em dispositivos.

3.47. Permitir que aplicativos gerenciados solicitem autenticação para execução.

3.48. Permitir o controle das funcionalidades e configurações de aplicativos baseando-se no perfil do usuário ou grupo de usuários.

3.49. Permitir o envio e o recebimento de notificações para o dispositivo móvel via método push.

3.50. Possuir console central de gerenciamento com suporte, ao idioma português Brasil.

3.51. Permitir o acesso total à console central de gerenciamento utilizando interface WEB.

3.52. Suportar o acesso à console central de gerenciamento, utilizando o protocolo HTTPS.

3.53. Suportar a configuração de acesso à console central de gerenciamento para grupos de usuários com permissões customizadas.

3.54. Possuir integração nativa com serviço de diretório LDAP do fabricante Microsoft (Active Directory).

3.55. Permitir a criação de políticas de gerenciamento aplicáveis a grupos do serviço de diretório do fabricante Microsoft (Active Directory).

3.56. Permitir a criação de políticas de gerenciamento específicas que se sobreponham às políticas definidas para um ou mais grupos de usuários existentes no serviço de diretório do fabricante Microsoft (Active Directory).

3.57. Possuir um portal de autosserviço web seguro (HTTPS) que possibilite aos usuários ativarem um conjunto limitado de ações nos dispositivos, ajustado por um administrador, reiniciarem a senha de acesso ao dispositivo, reiniciarem a senha dos dados e aplicativos corporativos (se houver uma), localizarem seus dispositivos em um mapa e fazer o wipe do conteúdo pessoal, corporativo ou total de seu dispositivo móvel.

3.57.1.1. O portal de autosserviço deverá ser acessível aos usuários tanto pela internet quanto pela rede local do CONTRATANTE, permitindo a autenticação e autorização pelo Microsoft Active Directory do CONTRATANTE;

3.57.1.2. O portal de autosserviço deverá consultar o Microsoft Active Directory somente se a conta de usuário for válida;

3.57.1.3. Após um número excessivo de tentativas de acesso com falha, o portal de autosserviço deverá apresentar um desafio (captcha) para o usuário preencher.

3.58. Permitir a proteção de conteúdo e caches de aplicações utilizando algoritmos de criptografia.

3.59. Permitir a criação de configuração de canal seguro de comunicação (VPN) no dispositivo móvel.

3.60. Permitir o bloqueio da função “copiar e colar” entre aplicações do dispositivo móvel, tais como, e-mail, textos, imagens, vídeos, dentre outros.

3.61. Permitir o bloqueio do envio de arquivos, conteúdos e informações pelo dispositivo móvel para aplicações não corporativas.

3.62. Permitir o bloqueio de compartilhamento de informações e conteúdo no dispositivo móvel, de aplicativos que estejam no container.

3.63. Permitir a emissão de relatórios nativos de inventário contendo no mínimo os seguintes:

3.63.1.1. Lista com o mapeamento de aplicativos instalados nos dispositivos móveis;

3.63.1.2. Lista de conformidade dos dispositivos móveis aderentes ou não às políticas configuradas na solução;

3.63.1.3. Lista com informações dos dispositivos móveis onde for identificada a ausência ou inoperância do agente da solução;

3.63.1.4. Permitir a geração de relatórios customizados baseados em filtros definidos a partir de qualquer informação coletada pelo inventário;

3.63.1.5. Permitir a geração de logs para fins de auditoria contendo no mínimo, as seguintes informações:

3.63.1.6. Nome do usuário;

3.63.1.7. Carimbo de data e horário (timestamp) do evento.

3.64. Permitir a integração nativa ou via componente com a ferramenta de SIEM - Security Information Event Management, para envio de logs em tempo real e agendado, dentre no mínimo dois padrões: ftp, csv, sftp, http, https nfs, cifs, wmi ou syslog; o CONTRATANTE reserva-se ao seu critério de utilizar tal integração.

3.65. Para o caso de integração via componente com a solução SIEM, o contratado deverá entregar, instalar, configurar e manter durante a vigência do contrato; o CONTRATANTE reserva-se ao seu critério de utilizar tal integração.

3.66. Permitir a criação de alertas automáticos quando o usuário executar uma ação específica no dispositivo móvel.

3.67. Possuir painel centralizado (dashboard) que permita a visualização periódica de informações coletadas nos dispositivos móveis.

3.68. Possuir relatórios analíticos de hardware e software referentes aos dispositivos móveis gerenciados.

3.69. Possuir relatórios analíticos no nível de aplicação (usuário executor, data e horário de execução etc.).

3.70. Além do ambiente de produção, a solução também deverá ser instalada em um ambiente de homologação.

3.71. Permitir a integração nativa com Microsoft Exchange 2010 SP3, Exchange, Office 365, IBM Notes, Google Apps

3.72. Permitir acesso seguro ao conteúdo:

3.72.1.1. Integração com repositórios do tipo Box, CMIS, Google Drive, OneDrive, OneDrive for Business, OneDrive for Business ADFS, Network Share, Sharepoint, Sharepoint ADFS, Sharepoint WebDAV, Sharepoint Windows Auth, Sharepoint Personal (MySites), Sharepoint O365, Sharepoint O365 ADFS, Sharepoint O365 OAuth, WebDAV

3.72.1.2. Sincronismo de conteúdo entre desktop e dispositivos móveis

3.72.1.3. Compartilhamento de conteúdo via link com opção de senha de acesso, data de expiração e limite de download

3.72.1.4. Permitir envio de conteúdo com funcionalidade de DLP como marca d'agua, edição, criptografia e controle de acesso somente Online ou somente Offline

3.73. Suportar a configuração de mecanismo de alta disponibilidade de forma nativa.

3.74. Ser capaz de integrar-se e gerenciar, no mínimo, os seguintes sistemas operacionais móveis, independente da camada de hardware do dispositivo móvel:

3.74.1.1. Google Android 8.0 ou superior;

3.74.1.2. Windows desktop 10, 11 ou superior;

3.74.1.3. macOS 11.6 ou superior

3.74.1.4. Apple iOS 14 ou superior

3.75. Possuir ferramenta de orquestração de workflows de TI complexos, permitindo aplicar políticas de forma sequencial e condicional aos critérios aplicados.

3.76. Possuir uma interface moderna, baixa complexidade de código, baseado em tela (*canvas*), para gerenciamento dos recursos tais como dispositivos, aplicações, scripts, sensores e arquivos.

3.77. Construir políticas de conformidade (*compliance*) com automação, remediação e fluxo de trabalho (workflow) tais como:

3.77.1. Permitir ou negar aplicação.

3.77.2. GPS e cerca virtual (*geofencing*).

3.77.3. Controle da versão do Sistema Operacional (SO).

3.77.4. Escalação de conformidade.

3.78. Permitir que a console central de gerenciamento possua funcionalidade para controlar o inventário dos dispositivos móveis, sendo possível coletar e armazenar, no mínimo, as seguintes informações:

3.78.1. Nome do usuário;

3.78.2. Número da linha telefônica;

3.78.3. Informações de hardware e software do dispositivo móvel.

3.79. A console de gestão de dispositivo deverá ser disponibilizada em ambiente nuvem na modalidade software como serviço (SaaS) sendo permitido a instalação de componentes dentro de uma infraestrutura local a ser definido pelo contratante.

3.80. Permitir a configuração de proteção com senha de bloqueio de tela nos dispositivos móveis.

3.81. Permitir executar o reset da senha de bloqueio de tela remotamente nos dispositivos móveis.

3.82. Permitir a configuração de políticas de senha de bloqueio de tela com, no mínimo, as seguintes opções:

3.82.1. Senha obrigatória;

3.82.2. Tamanho mínimo da senha;

3.82.3. Senhas do tipo alfanuméricas;

3.82.4. Uso de caracteres especiais;

3.82.5. Tempo de expiração das senhas;

3.82.6. Histórico de senhas (proteção de reutilização de senhas);

3.82.7. Definição do tempo de inatividade para bloqueio da tela do dispositivo móvel;

3.82.8. Número máximo de tentativas de uso da senha até o seu bloqueio.

3.83. Permitir a execução de ações nos dispositivos móveis gerenciados quando da violação de uma ou mais políticas de segurança configuradas nos dispositivos móveis.

3.83.1. As ações devem ser comandadas por meio da console central de gerenciamento.

3.84. Permitir o registro de violações de políticas para fins de auditoria, alerta e suporte.

3.85. Permitir a criação de relatórios e dashboards customizados

3.86. Permitir suporte remoto aos dispositivos Android, Windows 10, macOS, iOS e Linux com suporte:

3.87. Visualização e controle remoto

3.88. Gerenciamento de arquivos e acesso à linha de comando

3.89. Gravação de sessão e desenho na tela

3.90. Colaboração e bate-papo de sessão

3.91. Acesso com e sem autorização do usuário

Experiência Analítica e Inteligência

3.92. Permitir criar relatórios customizados com detalhes da experiência do usuário, contemplando itens como:

3.92.1.1. Dados de integridade do dispositivo (mobile e/ou desktop).

3.92.1.2. Informações dos dispositivos coletados a partir de sensores (scripts) para coleta customizada de dados.

3.93. Informação sobre atualização de sistema operacional.

3.94. Acompanhar métricas de espaço de trabalho digital que impacta a experiência dos usuários.

3.95. Proativamente identificar problema.

3.96. Remediar ações nos dispositivos Windows, macOS, iOS e Android, de forma rápida e automatizada.

4. SERVIÇOS DE SUPORTE, DE ASSISTÊNCIA TÉCNICA E MANUTENÇÃO

4.1. Os componentes de *software* da solução deverão possuir suporte, assistência técnica e manutenção por 4 (quatro) anos, inclusas na subscrição, a partir do início da vigência do contrato;

4.2. Componentes de *software*: suporte, assistência técnica e manutenção para falhas de desenvolvimento ou outras ocorridas em condições normais de uso. O fornecedor deverá reparar as falhas para restabelecer a condição normal do ambiente;

4.3. O suporte, assistência técnica e manutenção devem permitir:

4.3.1. Atualização das subscrições, sem custo, para novas versões dos componentes da solução lançadas durante seu período de vigência;

4.3.2. Acesso a documentações online mantidos pelo fornecedor, tais como manuais, bibliotecas e fóruns, para conhecimento de informações técnicas, soluções de

problemas, casos de uso e outras informações de apoio às atividades de administração do ambiente e solução de problemas (*troubleshooting*).

4.4. O fornecedor deverá disponibilizar canal de comunicação por telefone, com atendimento prestado por profissional especialista em suporte técnico, em língua portuguesa, para atendimento de chamados de todos os níveis de criticidade. Deve haver ferramenta web para registro dos chamados, possibilitando a contabilização de prazos e o acompanhamento das informações sobre o atendimento;

4.5. O atendimento deve obedecer aos Níveis Mínimos de Serviço a seguir:

4.5.1. Severidade 1 (crítica): problema grave que impede a utilização do ambiente:

- Disponibilidade: 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
- Resposta Inicial: até 30 (trinta) minutos.

4.5.2. Severidade 2 (alta): problema de alto impacto que prejudica severamente a utilização do ambiente sem, no entanto, impedir a realização de atividades essenciais:

- Disponibilidade: 8 (oito) horas por dia, horário comercial, 5 (cinco) dias por semana;
- Resposta Inicial: até 4 (quatro) horas úteis.

4.5.3. Severidade 3 (média): problema de impacto parcial e não-crítico que não impede a realização de atividades essenciais:

- Disponibilidade: 8 (oito) horas por dia, horário comercial, 5 (cinco) dias por semana;
- Resposta Inicial: até 8 (oito) horas úteis.

4.5.4. Severidade 4 (baixa): problema de baixo ou nenhum impacto na utilização do ambiente. Tipicamente envolve dúvida sobre utilização, requisição de melhorias, solicitação de atualizações e correção de documentação:

- Disponibilidade: 8 (oito) horas por dia, horário comercial, 5 (cinco) dias por semana;
- Resposta Inicial: até 12 (doze) horas úteis.

4.6. O CONTRATADO prestará assistência técnica aos itens da solução durante a vigência do Contrato, sendo responsável por todos os serviços de manutenção preventiva e evolutiva da solução;

4.7. Será considerado como horário comercial o período compreendido entre as 8:00 horas e 18:00 horas, nos dias úteis. Para feriados locais ou nacionais, será analisado o nível de serviço dentro de cada evento.

4.8. Os pedidos de assistência técnica serão registrados na ferramenta de registro de demandas internas do CONTRATANTE (*Service Desk Manager* - SDM).

4.9. Deverá ser alocado para fins de sustentação, on-site, com regime 5x8, em dias úteis, durante toda a vigência deste contrato;

4.10. O CONTRATADO deverá disponibilizar, no mínimo, 1 (um) profissional especialista/certificado na solução que trabalhará nas dependências do CONTRATANTE, no Centro Administrativo Presidente Getúlio Vargas (CAPGV) em Fortaleza-CE, para atendimento às demandas, sendo responsável por, no mínimo, as seguintes atividades, dentro do horário comercial:

4.10.1. análise dos chamados registrados pelo CONTRATANTE no SDM para prestar atendimento ou redirecionar, caso o chamado não seja de sua alçada;

4.10.2. atendimento de suporte de primeiro nível, esclarecendo dúvidas de utilização da solução e diagnosticando possíveis problemas informados;

4.10.3. manter atualizados no SDM os detalhes do andamento dos chamados abertos;

4.10.4. Os serviços compreendem desenvolvimento e manutenção evolutiva das atividades de serviço técnico e novas configurações na infraestrutura de virtualização da CONTRATANTE, incluindo, mas não se limitando, aos serviços listados a seguir:

4.10.4.1. Manutenção evolutiva para integração das soluções contratadas;

4.10.4.2. Apoio nas definições do produto para composição de soluções;

4.10.4.3. Suporte em soluções que utilizem o produto;

4.10.4.4. Avaliações, diagnósticos e proposições de soluções de melhoria;

4.10.4.5. Geração de relatórios de vistoria e análise;

4.10.4.6. Apoio em implementações adicionais;

4.10.4.7. Alteração da configuração na solução de virtualização de aplicativos implantadas;

4.10.4.8. Workshops de conscientização de usuários;

4.10.4.9. Elucidação de dúvidas técnicas de ambiente e análise de erros;

4.10.4.10. Avaliação de desempenho e adequação de desempenho, melhorias nos ambientes, solução de possíveis incompatibilidades, parecer técnico e configurações recomendadas de melhores práticas;

4.10.4.11. Dúvidas e suporte sobre regras gerais e inclusão de recursos correlacionados;

4.10.4.12. Transferência de Conhecimento.

4.10.5. As atividades deverão ser atendidas e executadas em função do seu nível de complexidade. Dada a sua variação, deverá ser disponibilizado o profissional com o nível de conhecimento adequado e proporcional ao nível de complexidade da atividade.

4.10.6. A complexidade das atividades considera a relevância dos serviços, sua precedência sobre as demais, sua dificuldade operacional, o grau de documentação existente, as características dos profissionais de mercado e sua capacidade em cumprir as atividades.

4.10.7. Todos os serviços devem ser executados e documentados obedecendo aos critérios estabelecidos em metodologia a ser indicada pelo CONTRATADO e referendada pelo CONTRATANTE.

4.10.8. O atendimento as demandas de manutenção evolutiva deverão ter seu início através de acordo entre as partes, salvo quando for identificada uma das severidades relacionadas mais abaixo nesse texto.

4.11. Para a equipe residente do CONTRATADO, o CONTRATANTE disponibilizará espaço físico com computador, telefone e acessos a Internet e ferramenta de registro de demandas internas do CONTRATANTE (*Service Desk Manager*).