ANEXO I - ESPECIFICAÇÃO TÉCNICA

Contratação de empresa especializada para o fornecimento de **Solução de Gerenciamento de Acessos Privilegiados (*Privileged Access Management – PAM*)**, e demais serviços associados.

1. ITEM 01 - SOLUÇÃO DE GERENCIAMENTO DE ACESSOS PRIVILEGIADOS (PAM)

1.1. REQUISITOS GERAIS

1.1.1. A solução de gerenciamento de acessos privilegiados deverá ser implementada em modo cluster de alta disponibilidade, com capacidade para armazenar e gerir credenciais com acessos privilegiados, descoberta das credenciais nos sistemas-alvo, duplo fator de autenticação, e as demais especificações constantes neste termo de referência.

1.1.2. A solução deve possuir todos os módulos e funções fornecidos pelo mesmo fabricante, sem dependência de ferramentas de terceiros ou adaptações, com exceção para o módulo com as funcionalidades de duplo fator de autenticação que poderá ser de outro fabricante.

1.1.3. Deve possuir interface única, na mesma solução, para o gerenciamento de contas, senhas, sessões e ativos agregados ao cofre de senhas.

1.1.4. O acesso ao módulo de gerenciamento e ao portal deverá ser baseado em web, utilizando HTML5 e através de HTTPS (Secure Hypertext Transfer Protocol). Devendo ainda, ser compatível, minimamente, com os navegadores Microsoft Edge (baseado em Chromium), Google Chrome e Mozilla Firefox.

1.1.5. A solução deverá prover mecanismos de atualização de segurança, de forma automática ou sob demanda.

1.1.6. Não depender da instalação de agentes para realizar a troca de senhas e gravação de sessão.

1.1.7. A solução deve estar licenciada para atender aos quantitativos descritos na tabela a seguir:

Item	Descrição	Quantidade
1	Dispositivos de rede: LAN, WAN, WI-FI, Firewall, IPS, AntiSpam, ADC, hipervisor, storage etc.	360
2	Servidores Windows	200
3	Servidores Linux	500
4	Usuários com perfil privilegiado	200
5	Estações de trabalho Windows	200
6	Instâncias de Banco de Dados	50
7	Instâncias de aplicações/serviços corporativos/senhas hardcoded	250

1.1.8. A solução de gerenciamento de acesso privilegiado, bem como os

componentes necessários para o funcionamento deverão ser instalados e executados na infraestrutura do MPDFT, com fornecimento de todos os softwares necessários para operação, incluindo todas as licenças necessárias.

1.1.8.1. A Instalação deverá ser em appliance virtual em formato compatível com a plataforma VMware ou instalado diretamente em sistema operacional Windows ou Linux.

1.1.8.2. A CONTRATANTE irá fornecer os recursos de armazenamento e processamento necessários para a implantação da solução no ambiente de virtualização VMware.

1.1.8.3. Caso a solução necessite de outros softwares para seu funcionamento, como Sistema Gerenciador de Banco de Dados, Geradores de Relatórios etc., as licenças desses softwares deverão ser fornecidas no bojo da solução, sem ônus para o CONTRATANTE.

1.1.9. A solução deverá, minimamente, suportar a conexão simultânea dos usuários com perfil privilegiado indicados no quadro anterior, com todas as funcionalidades habilitadas.

1.1.10. Tanto appliances virtuais quanto sistemas operacionais devem ser "hardenizados" e protegidos com firewall interno;

1.1.11. Utilizar um banco de dados com as melhores práticas de segurança, devendo estar em ambiente "hardenizado", com mecanismo de blindagem e criptografia do sistema operacional e documentação que comprove a contemplação destes requisitos.

1.1.12. Permitir o backup e o recovery de seu banco de dados, bem como das configurações de software estabelecidas, com as seguintes capacidades:

1.1.12.1. Permitir a execução de tarefas de backup e criptografia sem a necessidade de agentes de terceiro, provendo assim o maior nível possível de segurança e integridades dos dados a serem copiados;

1.1.12.2. Permitir a execução de Backups automatizados por meio de programação/agendamento de horários;

1.1.12.3. Permitir a salvaguarda do arquivo de backup criptografado em diretório compartilhado.

1.1.13. Possibilitar a utilização de criptografia do banco de dados utilizado pela solução, para armazenar as senhas das credenciais gerenciadas por ela, devendo ainda ser compatível com pelo menos um dos seguintes métodos e padrões de criptografia:

1.1.13.1. AES com chaves de 256 bits;

1.1.13.2. FIPS 140-2;

1.1.13.3. Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo fabricante para a solução ofertada;

1.1.14. Prover autenticação transparente no sistema-alvo ou dispositivo de rede. A solução deve iniciar uma sessão injetando diretamente as credenciais na tela de login e servindo como um proxy para a sessão entre o usuário e o sistema-alvo, de forma que a senha não seja exposta ao solicitante do acesso;

1.1.15. Não permitir a abertura do cofre com chaves criptográficas geradas por seus respectivos fornecedores e/ou fabricantes em hipótese alguma.

1.1.16. A CONTRATADA será responsável pelas atualizações, configurações de segurança e performance, atualização de firmwares e componentes de hardware enquanto durar o contrato.

1.1.17. Ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos.

1.1.18. Permitir, através de interface gráfica, que administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.

1.1.19. A solução deve possuir ferramenta de monitoração própria para que seja possível especificar limiares (threasholds) referente ao uso de memória, CPU, disco e banco de dados, por exemplo.

1.1.19.1. Caso não possua ferramenta de monitoração própria, a CONTRATADA deverá fornecer as informações de monitoramento, via SNMP, de quais itens devem ser monitorados com seus respectivos limiares.

1.1.20. Implementar em sua interface web e de administração suporte a autenticação de duplo fator.

1.1.21. Os produtos utilizados devem possuir licenciamento integral para todas as funcionalidades especificadas neste termo de referência. Caso alguma funcionalidade não tenha sido especificada neste documento, mas é abarcada no critério de licenciamento do fabricante, a CONTRATANTE poderá fazer uso dela, inclusive com a respectiva garantia.

1.1.22. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução.

1.1.22.1. Caso a solução não possua licenciamento perpétuo, deverá permanecer com todas as funcionalidades ativas por pelo menos seis meses após o término da garantia.

1.1.23. A solução deverá permitir a migração de licenças entre endereços IP distintos.

1.1.24. Os produtos que compõem a solução deverão ter seu funcionamento restrito às suas funções, não podendo interferir ou causar lentidão no funcionamento das redes locais das unidades do CONTRATANTE.

1.1.25. Assume-se que todos os itens descritos neste termo de referência estarão contemplados na solução independente de qual módulo da solução implementa a funcionalidade e do verbo aplicado ao item.

1.1.26. Todos os equipamentos, produtos, peças ou softwares necessários à implementação da solução devem ser novos e de primeiro uso, não deverão constar, no momento da apresentação da proposta, em listas de *end-of-sale*, *end-of-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Os produtos utilizados devem possuir licenciamento, garantia do fabricante e atualização de versão pelo período de 5 anos.

1.2. ARQUITETURA DA SOLUÇÃO

1.2.1. A solução deverá ser implementada em modo cluster de alta disponibilidade.

1.2.2. A solução deve atender o conceito de tolerância a falhas e não ter restrições para funcionar em modo de alta disponibilidade ativo/passivo.

1.2.3. Implementar alta disponibilidade ativo/passivo para todos os componentes que fazem parte da solução, onde na falha do nó primário, o nó secundário deve assumir suas funções automaticamente permitindo a continuidade do acesso as contas privilegiadas.

1.2.4. Permitir que os controles sejam feitos via interface gráfica, sem depender de comandos manuais, scripts ou adaptações.

1.2.5. Manter sincronização de dados e versões de aplicação entre os nós, sendo gerenciada nativamente pela solução sem necessidade de intervenção manual para a garantia de sincronia.

1.2.6. Os nós devem ter mecanismo de backup/restore próprio para realização de ações de recuperação de desastres em caso de catástrofe, permitindo ainda a salvaguarda dos arquivos em diretório compartilhado.

1.3. DUPLO FATOR DE AUTENTICAÇÃO

1.3.1. A solução deverá prover módulo de duplo fator de autenticação para ser utilizado pelos usuários com perfil privilegiado.

1.3.2. Permitir a utilização em dispositivos móveis, devendo ser compatível, minimamente, com os sistemas operacionais android e ios.

1.3.3. Prover como um dos fatores de autenticação:

1.3.3.1. Biométrico, tais como a detecção de vivacidade (através da face, íris ou da voz) e identificação por digital;

1.3.3.2. Notificações por "*push*" para autenticação com um clique, possibilitando ao usuário pressionar um "*ok*" em seu dispositivo móvel.

1.3.3.3. Senhas de uso único – OTP, com validade em um certo período.

1.3.4. O módulo deve ainda realizar a verificação do dispositivo móvel em que está instalado e alertar ou limitar o acesso em caso de risco do dispositivo. O risco deve ser mensurado pelos seguintes fatores (rol exemplificativo):

1.3.4.1. Atualização do sistema operacional do dispositivo (versão mínima segura);

1.3.4.2. Atualização do módulo de autenticação (versão mínima segura);

1.3.4.3. Verificar se o dispositivo móvel possui mecanismos de bloqueio de tela e desbloqueio por código/biometria habilitados;

1.4. DESCOBERTA DE USUÁRIOS PRIVILEGIADOS E CHAVES SSH

1.4.1. Ter a capacidade de realizar a descoberta de informações sobre as contas de ativos na rede trazendo, no mínimo, informações sobre o tipo de conta (privilegiada ou padrão).

1.4.2. Minimamente suportar a adição de contas privilegiadas em:

1.4.2.1. Windows: 10, Server 2012 R2, Server 2019, e superiores;

1.4.2.2. Linux: Debian 9 e 10, Ubuntu 18, 19 e 20, CentOS 7, e superiores;

1.4.2.3. Banco de dados: SQL Server 2016, Oracle 18c, e superiores;

1.4.3. Identificar contas privilegiadas com ID 0 ('0') no Linux e as contas que não possuem ID zero, porém, são privilegiadas através do uso de ´sudo´ (configuradas no Sudoers).

1.4.4. Permitir a criação de conjuntos de permissões automáticas de acordo com ativos descobertos;

1.4.5. Possuir mecanismos de alerta no descobrimento de novos ativos ainda não

agregados ao cofre;

1.4.6. Possuir a capacidade de descobrimento de chaves SSH em servidores Linux.

1.5. GERENCIAMENTO DE SENHAS E USUÁRIOS PRIVILEGIADOS

1.5.1. Possuir integração com o Active Directory para delegação de acesso aos servidores gerenciados;

1.5.2. Suportar o gerenciamento de contas privilegiadas no mínimo nos seguintes sistemas/aplicações, através de conector padrão, conectores customizados ou integração via API:

1.5.2.1. Windows: 10, Server 2012 R2, Server 2019, e superiores;

1.5.2.2. Linux: Debian 9 e 10, Ubuntu 18, 19 e 20, CentOS 7, e superiores;

1.5.2.3. Banco de dados: SQL Server 2016, MySQL 5.6, Oracle 18c, e superiores;

1.5.2.4. Ativos de rede: Sophos XG Firewall, f5 BIG-IP, Roteadores Cisco e Switches Dell

1.5.2.5. Servidores de aplicação e servidores WEB: Microsoft IIS, JBoss, Apache Tomcat;

1.5.2.6. Hipervisores VMware e Citrix XenServer;

1.5.3. Garantir a aplicação apenas dos privilégios adequados, provendo acesso às senhas das contas privilegiadas ao pessoal autorizado;

1.5.4. Possibilitar a criação de novos conectores baseado em acessos via Telnet, SSH e API Rest, para que seja possível suportar novas plataformas;

1.5.5. Permitir a configuração da política de formação e troca de senha;

1.5.6. Permitir a troca de senha de forma automática após cada uso, protegendo-as por meio de regras de complexidade que incluem comprimento da senha (quantidade de caracteres), frequência de troca da senha, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas;

1.5.7. Possuir sistema para definição de fluxos de aprovação para requisições de acesso a credenciais privilegiadas, com notificação aos aprovadores via e-mail e notificação pela interface da ferramenta;

1.5.8. Permitir configurar o fluxo de aprovação para ter dois ou mais aprovadores antes de liberar acesso a uma credencial privilegiada;

1.5.9. Permitir acesso imediato as contas privilegiadas e em data futura aos requisitantes;

1.5.10. Permitir a criação de políticas de acesso atribuída aos requisitantes, possibilitando por exemplo: configurar se haverá necessidade de aprovação ou não do acesso; definir se o usuário poderá ver a senha ou somente realizar uma sessão RDP/SSH.

1.5.11. Gestão automática de chaves SSH (rotação das chaves, fluxo de aprovação etc.), para os usuários que acessam servidores Linux via chaves SSH com suporte a ´passphrases´;

1.5.12. Possuir uma política para realizar a rotação das chaves SSH de acordo em uma determinada frequência: Diariamente, mensalmente, trimestralmente etc.

1.5.13. Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda, realizando verificações agendadas e automáticas a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino, correspondam às mesmas senhas armazenadas no banco de dados da solução;

1.5.14. Caso a senha da conta gerenciada pela solução seja diferente daquela armazenada no banco de dados, a solução deve ser capaz de gerar relatórios e alertas do evento;

1.5.15. Permitir o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;

1.5.16. Permitir efetuar a troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido;

1.5.17. Permitir a troca de senhas nos sistemas gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (Grupo de Todos os Sistemas Operacionais LINUX, por exemplo);

1.5.18. Possuir controle de acesso baseado em papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada;

1.5.19. Garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial;

1.5.20. Possuir portal de acesso, permitindo aos solicitantes selecionar os servidores nos quais possuem autorização e realizar a inicialização da sessão RDP ou SSH;

1.5.21. Possuir mecanismo para permitir o acesso de contas privilegiadas sem

revelar a senha e sem depender do portal de acessos, ou seja, os usuários devem a partir de clientes comuns (RDP/putty) iniciar um acesso direto ao cofre de senhas e ele direcionar o acesso aos servidores gerenciados, realizando a submissão da solicitação de acesso e aprovação automaticamente;

1.6. GRAVAÇÃO E GERENCIAMENTO DE SESSÕES

1.6.1. Incluir o suporte para gerenciamento de sessões RDP e SSH, sem depender de integrações com ferramentas de terceiros;

1.6.2. Implementar controle de acesso às sessões gravadas e às sessões que estão sendo realizadas em tempo real, permitindo a atribuição de auditoria de determinadas sessões a determinados grupos ou pessoas autorizadas.

1.6.3. Gravar sessões RDP e SSH e permitir a reprodução por um auditor para efeito de auditoria;

1.6.4. Permitir que a busca de registro da sessão seja realizada, minimamente, por usuário, sistema-alvo, endereço IP, data e hora.

1.6.5. Permitir a busca de comandos e tudo que foi digitado em uma determinada sessão ou em várias sessões, a fim de facilitar o trabalho do auditor e de identificar todas as sessões onde um determinado comando foi executado;

1.6.6. Permitir o monitoramento de sessões, possibilitando identificar, em tempo real, todas as atividades realizadas por um determinado administrador, permitindo inclusive que um administrador possa terminar uma sessão ativa;

1.6.7. Possuir a função de bloqueio de comandos digitados pelos usuários em sessões SSH;

1.6.8. Possuir mecanismo de compactação e/ou otimização do espaço de armazenamento das sessões gravadas;

1.6.9. Ter capacidade de armazenar na solução as sessões gravadas por, no mínimo, seis meses;

1.6.10. Permitir a exportação das gravações para armazenamento fora da solução, podendo importar as sessões por demanda do auditor.

1.7. ACESSO REMOTO SEGURO

1.7.1. A solução deverá ser entregue com acesso remoto seguro (externo a rede corporativa), sem a necessidade de entrega de credenciais, sem instalação e uso de clientes e VPN nos dispositivos dos usuários remotos;

1.7.2. O acesso remoto seguro deverá ser realizado pelos usuários com perfil privilegiado nas suas respectivas estações de trabalho.

1.7.3. Deverá ser disponibilizado ao usuário com perfil privilegiado um acesso baseado em web, utilizando HTML5 e através de HTTPS, com suporte a autenticação de duplo fator;

1.7.4. Deverá estar integrado ao cofre de senhas;

1.7.5. Deverá suportar a injeção automática de credenciais, permitindo que os usuários autentiquem nos sistemas remotos, sem revelar credenciais. Permitindo que os usuários selecionem a credencial a ser utilizada a partir de lista de credenciais que têm privilégios nos sistemas aprovados para acesso;

1.8. RELATÓRIOS

1.8.1. Oferecer opção de criar relatórios personalizados, além dos relatórios já embutidos na solução e relatórios de auditoria;

1.8.2. Possuir relatórios pré-definidos com pelo menos as seguintes informações:

1.8.2.1. Idade de senhas das contas: o relatório deve fornecer uma lista de contas de usuário habilitadas das quais as senhas não foram alteradas em mais de 30 dias;

1.8.2.2. Atividade: o relatório deve fornecer um histórico detalhado de todas as alterações de segurança de senha feitas nos dispositivos por qualquer usuário;

1.8.2.3. Lista de contas gerenciados pelo cofre: o relatório deve fornecer uma lista de todas as contas gerenciadas pelo cofre juntamente com os detalhes da idade da senha;

1.8.2.4. Lista de contas gerenciadas e não gerenciadas: o relatório deve fornecer uma lista com detalhes de conta de usuário de ativos, filtrados por localização, status, associação de grupo e mais;

1.8.2.5. Atividade de senhas e sessões: o relatório deve fornecer uma visualização transacional detalhada das atividades de sessão do cofre;

1.8.2.6. Atividade de liberação de senha: o relatório deve fornecer uma lista detalhes da atividade de liberação de senha do cofre;

1.8.2.7. Atividade de atualização de senha: o relatório deve fornecer os detalhes da atividade de atualização de senhas;

1.8.2.8. Programação de atualização de senha: o relatório deve fornecer os detalhes das próximas atualizações de senhas programadas;

1.8.2.9. Troca de senhas: o relatório deve fornecer provas auditáveis de que as senhas das contas privilegiadas armazenadas no cofre de senhas foram

reiniciadas adequadamente após serem utilizadas;

1.8.3. Deverá ser possível a realização de filtros nos relatórios, minimamente, por período, usuário e sistema-alvo;

1.8.4. Permitir a exportação dos relatórios para, no mínimo, um dos seguintes formatos: PDF, CSV e HTML;

1.9. GERENCIAMENTO DE USUÁRIOS EM APLICAÇÕES

1.9.1. Permitir a gestão de senhas no código fonte em aplicações e scripts;

1.9.2. Ser disponibilizada com um SDK (Software Development Kit) ou API (Application Programming Interface) que pode ser configurado para permitir que aplicações possam:

1.9.2.1. Solicitar as credenciais sob demanda ao invés de utilizar credenciais estáticas; e

1.9.2.2. Atualizar informações de contas automaticamente no banco de dados de senhas.

1.9.3. Possuir API para que as aplicações utilizem a senha com requisições a interface REST, assim evitando que as senhas fiquem expostas no código fonte das aplicações. A interface REST deve ser extensível com suporte a várias linguagens como: Perl, PHP, .NET e Java;

1.9.4. Possuir controles de segurança extensivos que bloqueiam o acesso, permitindo somente a aplicativos autorizados.

1.10. GARANTIA DA SOLUÇÃO LICENCIADA E ATUALIZAÇÃO DE VERSÃO:

1.10.1. A solução deverá ter garantia de 5 anos, para equipamentos, produtos e seus componentes, sem quaisquer ônus para a CONTRATANTE, a contar da data de emissão do Termo de Homologação, estendendo-se por todo o período de vigência do contrato. Subdivide-se em:

1.10.1.1. Garantia técnica evolutiva: fornecimento de novas versões e / ou releases corretivos de softwares, lançadas durante a vigência do contrato, mesmo em caso de mudança de designação do nome. A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem. Inclui também, implementações de novas funcionalidades relativas aos equipamentos e produtos;

1.10.1.2. Garantia técnica corretiva: série de procedimentos executados para recolocar a solução em seu perfeito estado de uso, funcionamento e

desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

1.10.1.3. Garantia Técnica proativa: Manutenções proativas pré-acordadas entre CONTRADADA e CONTRATANTE para execução de análises, ações e correções que visem preservar funcionamento e otimizar desempenho dos equipamentos e produtos, seguindo melhores práticas recomendadas pela fabricante

1.10.1.4. Garantia técnica assistencial: atividades que incluem, mas não se limitam a execução e provimento de informação, assistência e orientação para: instalação, desinstalação, configuração, substituição e atualização de programas (software) e dispositivos físicos (hardware); aplicação de correções (patches) e atualizações de software; diagnósticos, avaliações e resolução de problemas; ajustes finos e customização da solução; esclarecimento acerca das características dos produtos; e demais atividades relacionadas à correta operação e funcionamento da solução da melhor maneira possível.

1.10.2. A CONTRATADA deverá entregar documentação comprobatória da contratação da Garantia Técnica junto ao fabricante da solução ofertada;

1.10.2.1. A Garantia Técnica deverá ser em nome da CONTRATANTE;

1.10.2.2. A contratação da garantia técnica junto ao fabricante não exime a CONTRATADA das responsabilidades contratuais;

1.10.2.3. A Garantia Técnica deverá ser prestada pelo fabricante dos equipamentos e produtos ou pela rede de assistência técnica autorizada que o represente, sempre sob responsabilidade da CONTRATADA.

1.10.3. A CONTRATADA deverá apresentar soluções definitivas para os problemas relatados e identificados por solicitação de garantia técnica pelo CONTRATANTE, dentro dos prazos e condições estabelecidos neste Termo de Referência;

1.10.4. A CONTRATADA prestará a garantia técnica on-site, remotamente ou por telefone sempre que se fizer necessário ou quando solicitado pelo CONTRATANTE. O tipo de atendimento será definido pela equipe técnica do CONTRATANTE;

1.10.5. A CONTRATADA deve disponibilizar Central de Atendimento para a abertura e fechamento de chamados de garantia técnica, conforme períodos e condições estabelecidas neste Termo de Referência;

1.10.6. A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço de atendimento telefônico com discagem gratuita 0800 ou de custo local fixo

e, adicionalmente, sítio Web ou e-mail, sem ônus adicional para a CONTRATANTE, para abertura e acompanhamento de chamados. É imprescindível que os funcionários de atendimento da CONTRATADA conheçam a solução CONTRATADA e estejam aptos a dar as informações básicas sobre a solução;

1.10.7. Os chamados provenientes dessa contratação deverão ter acesso prioritário à especialistas nas áreas técnicas convenientes

1.10.8. Os chamados abertos deverão ter acompanhamento de um Gerente de Serviços de TI

1.10.8.1. O gerente de serviços de TI deverá atuar no acompanhamento dos chamados, garantindo total atendimento dentro do Acordo de Nível de Serviço definido

1.10.9. Quando aplicável, serão emitidas em conjunto com o fechamento de chamados avaliações e sugestões de melhores práticas e ajustes do ambiente de TI do CONTRATANTE

1.10.10. A Garantia Técnica deverá, ao ser acionada, registrar o chamado, protocolar a data e hora da solicitação, nome do SOLICITANTE e descrição detalhada da solicitação;

1.10.11. A CONTRATADA encaminhará mensagem de e-mail para endereço a ser indicado pelo CONTRATANTE informando o número de protocolo do chamado técnico, data e hora de abertura e sua descrição;

1.10.12. O serviço de abertura de chamados para a garantia deverá ser realizado em regime de 24x7 (vinte e quatro horas por dia, sete dias por semana), todos os dias do ano, no idioma português, incluindo o atendimento telefônico, o e-mail e o sítio Web;

1.10.13. A critério do CONTRATANTE, o atendimento às solicitações deverá ser realizado nas instalações do CONTRATANTE (on-site) e não poderá ser interrompido até o completo reestabelecimento dos equipamentos e da solução, mesmo que se estenda por períodos noturnos, sábados, domingos e feriados, salvo acordo prévio e expresso com a CONTRATANTE. Também não implicará em custos adicionais ao CONTRATANTE;

1.10.14. A interrupção do atendimento por parte da CONTRATADA e sem a prévia autorização da equipe técnica do CONTRATANTE poderá ensejar na aplicação das penalidades previstas;

1.10.15. Deverá haver uma descrição da solução, imediatamente após fechamento dos chamados, acerca das soluções aplicadas para definitivamente retornar a solução ao pleno estado de funcionamento. Essa descrição deverá fornecer em detalhes, por e-mail ou via sítio Web, a solução para o problema detectado. Deverá cobrir todo e qualquer defeito apresentado no serviço,

incluindo todos os componentes da solução, equipamentos de comunicação, peças e esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias;

1.10.16. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componentes da solução, essa deverá ocorrer sem custo adicional para o CONTRATANTE;

1.10.17. No caso de substituição temporária, o equipamento, peça e componente deverá possuir, no mínimo, características técnicas e desempenho iguais ou superiores às substituídas com a anuência do CONTRATANTE.

1.10.18. A substituição temporária do equipamento, peça e componente será por até 30 dias, ficando suspensa a contagem do prazo de solução definitiva;

1.10.19. A CONTRATADA substituirá, no prazo de 10 dias, qualquer equipamento que venha a se enquadrar em, pelo menos, um dos seguintes casos:

1.10.19.1. Indisponibilidade ocasionada por componente defeituoso que não tenha sido substituído no prazo de até 4 (quatro) dias corridos;

1.10.19.2. Ocorrência de 3 (três) ou mais substituições de um mesmo componente do equipamento dentro de um período contínuo de 60 (sessenta) dias corridos;

1.10.19.3. Se a soma dos tempos de indisponibilidade de um mesmo componente ultrapassar 48 (quarenta e oito) horas dentro de um período contínuo de 90 (noventa) dias corridos;

1.10.19.4. Se a soma dos tempos em que o equipamento apresentar indisponibilidade total, comprometimento de performance ou de funcionalidade ultrapassar 48 (quarenta e oito) horas dentro de um período contínuo de 60 (sessenta) dias corridos.

1.10.20. No caso de substituição definitiva, o equipamento, peça e componente deverá possuir, no mínimo, características técnicas e desempenho iguais ou superiores às substituídas, serem novas e de primeiro uso;

1.10.21. O envio para centros de Garantia técnica em outra localidade não exime a CONTRATADA do cumprimento dos prazos estabelecidos nos níveis de serviço exigidos;

1.10.22. Para a remoção de equipamento, peça e componente será necessária autorização de saída emitida pelo Fiscal do Contrato, a ser concedida ao funcionário da CONTRATADA, formalmente identificado.

1.10.23. A CONTRATADA deve prover as correções e atualizações mais recentes dos hardwares instalados, tais como firmware, que permitam melhorar as

funcionalidades dos equipamentos e mantê-los compatíveis com os demais componentes de hardware e software do parque tecnológico do MPDFT, sem ônus adicional para ao CONTRATANTE;

1.10.24. A CONTRATADA deve prestar as informações e/ou esclarecimentos que venham a ser solicitados pela equipe técnica do CONTRATANTE referente a qualquer problema detectado ou sobre o andamento das atividades de manutenção;

1.10.25. A CONTRATADA deve assegurar a Garantia Técnica necessária ao perfeito funcionamento dos equipamentos e produtos que compõem a solução, efetuando ajustes, reparos ou substituição parcial ou total dos equipamentos, peças e partes sob sua propriedade e responsabilidade, sem ônus adicionais para o CONTRATANTE.

1.10.26. Todas as despesas decorrentes da necessidade de substituição de equipamentos, infraestrutura, transporte, deslocamento, embalagem, peças, partes, manuais do fabricante, serão de inteira responsabilidade da CONTRATADA, não devendo gerar qualquer ônus adicional à CONTRATANTE;

1.10.27. A CONTRATADA responderá por quaisquer prejuízos que seus empregados causarem ao patrimônio do CONTRATANTE ou a terceiros, por ocasião da prestação dos serviços, procedendo imediatamente os reparos ou indenizações cabíveis e assumindo o ônus decorrente.

1.10.28. A CONTRATADA arcará com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a ser devidos em decorrência da execução CONTRATADA, bem como custos relativos ao deslocamento e estada de seus profissionais, caso exista.

1.10.29. Oferecer serviço e ferramentas de diagnóstico e troubleshooting remotos na qual os técnicos da CONTRATADA se conectam diretamente ao sistema do usuário através de uma conexão de Internet segura para agilizar e melhorar o processo de solução de problemas;

1.10.30. A CONTRATADA se compromete a utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações neste Termo de Referência.

1.10.31. Os chamados técnicos serão categorizados nas severidades Alta, Média e Baixa, devendo ser atendidos nos prazos especificados neste edital nos Níveis Mínimos de Serviço Exigidos (NMSE).

1.10.32. Serão considerados, para efeito do nível de serviço exigido:

1.10.32.1. Término do atendimento: Tempo decorrido entre a abertura do chamado pela CONTRATANTE e a solução definitiva da demanda pela

CONTRATADA.

1.10.33. O atendimento da demanda só será considerado concluído após o aceite formal da equipe técnica da CONTRATANTE. Caso a CONTRATANTE não confirme a conclusão do atendimento, este permanecerá aberto. Nesse caso, a CONTRATANTE fornecerá informações sobre as pendências a serem resolvidas;

1.10.34. A severidade do chamado será informada pela CONTRATANTE no momento da sua abertura e seguirá o disposto na tabela I;

1.10.35. A severidade poderá ser reclassificada pela CONTRATANTE. Caso isso ocorra, haverá nova contagem de prazo, conforme a nova severidade e seguirá os prazos dispostos na tabela II;

1.10.36. É vedado à CONTRATADA interromper o atendimento de severidade ALTA até que o equipamento esteja em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. Ainda assim, não haverá custos adicionais à CONTRATANTE.

1.10.37. É necessária autorização da CONTRATANTE para qualquer modificação na solução;

1.10.38. A CONTRATADA será a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a garantia;

1.10.39. A CONTRATADA deverá ser parceira autorizada do fabricante estando apta e autorizada a fornecer o objeto, conforme Termo de Referência.

2. ITEM 02 – SERVIÇOS DE IMPLANTAÇÃO, INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO CONTRATADA.

2.1. Para todo o produto (hardware ou software) adquirido no escopo do ITEM 1 deverá ser fornecido serviço especializado de instalação, customização e configuração da solução contratada no ambiente do MPDFT. Entende-se por serviço especializado de instalação, customização e configuração a montagem física dos equipamentos e seus respectivos acessórios pela CONTRATADA, bem como a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com a necessidade do MPDFT.

2.2. A implantação deverá ser realizada por profissionais certificados e qualificados para customizar as ferramentas às necessidades do MPDFT, devendo ter a orientação profissional do fabricante da solução nas atividades de elaboração do projeto de implantação dos casos de uso da solução e na validação da configuração feita durante a implantação.

3. ITEM 03 - TRANSFERÊNCIA DE CONHECIMENTO

3.1. Para todo o produto adquirido no escopo do ITEM 1 deverá ser fornecida uma transferência de conhecimento.

3.2. A transferência de conhecimento deverá ser ministrada por profissional certificado pelo fabricante.

3.3. A CONTRATADA deverá apresentar um Plano de Transferência de Conhecimento que será avaliado e aprovado pela equipe técnica da CONTRATANTE;

3.4. O Plano citado no item anterior deverá apresentar o programa de cada transferência de conhecimento com conteúdo, carga horária, duração em dias e avaliações de aprendizagem;

3.5. A transferência de conhecimento pode ser pela manhã, manhã e tarde, ou de noite, a critério da CONTRATANTE;

3.6. A transferência de conhecimento deverá ser em cada uma das ferramentas, contemplando módulos, com conteúdo teórico e prático, com programas mínimos que abordem toda a instalação, configuração e utilização delas;

3.7. A transferência de conhecimento deverá prever a capacitação para 6 alunos divididos em 2 turmas;

3.8. Para que uma transferência de conhecimento seja considerada efetiva deverá ser considerada satisfatória por pelo menos 70% dos treinandos;

3.9. A CONTRATANTE poderá avaliar as transferências de conhecimentos com meios próprios e, caso este seja julgado deficiente, a CONTRATADA deverá prover o devido reforço;

3.10. A CONTRATADA deverá prover toda a estrutura para as transferências de conhecimentos;

3.11. A transferência de conhecimento será realizada na modalidade de ensino a distância (EAD);

3.11.1. Em casos excepcionais a serem julgados pela CONTRATADA a transferência de conhecimento poderá ser realizada presencialmente em Brasília.

3.12. Todo material didático disponibilizado na transferência de conhecimento deverá ser fornecido pela CONTRATADA e estarão inclusos no escopo da transferência de conhecimento;

3.13. Ao final de cada transferência de conhecimento, cada treinando deverá receber um certificado de participação;

3.14. No certificado de participação de que trata o item anterior deverá constar todas as informações exigidas pela Secretaria de gestão de pessoas do MPDFT para que o mesmo seja homologado. Minimamente, mas não limitado a: nome completo do aluno, data de execução da transferência de conhecimento, carga horária e ementa do curso;

3.15. A CONTRATADA arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades da transferência de conhecimento;

3.16. A fim de que os técnicos da CONTRATANTE possam avaliar com precisão a solução durante o Período de Funcionamento Experimental (PFE), ao menos uma turma da transferência de conhecimento deve ser finalizada antes do início deste.

4. ITEM 04 – SERVIÇO DE SUPORTE TÉCNICO MENSAL

4.1. Entende-se como Suporte Técnico: o monitoramento, operação, administração e assistência técnica de todos os componentes da solução fornecidos pela CONTRATADA;

4.2. O Suporte Técnico deve estar totalmente funcional no início do Período de Funcionamento Experimental – PFE, estendendo-se por todo o período de vigência do Contrato;

4.3. Os serviços deverão ser prestados preferencialmente de forma remota;

4.4. O Suporte Técnico deverá cobrir a localidade de Brasília/DF;

4.5. O suporte técnico operará ininterruptamente, 24 horas por dia, 7 dias por semana, 365 dias por ano;

4.6. Sem apresentar qualquer ônus adicional à CONTRATANTE, o Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado incluindo, mas não se limitando a esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias, acionar a garantia do produto para substituição total ou parcial do produto como peças, partes, componentes ou acessórios;

4.7. A CONTRATANTE poderá, a qualquer momento, determinar à CONTRATADA a execução de rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos;

4.8. Serviços de assistência técnica deverão ser executados pela CONTRATADA sempre que se fizer necessário, independentemente de haver solicitação por parte da CONTRATANTE;

4.9. A realização de assistência técnica preventiva deverá ser combinada entre as partes com antecedência mínima de 2 dias úteis, devendo o horário ser negociado

de forma a não haver impacto no ambiente de produção da CONTRATANTE;

4.10. A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho;

4.11. A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

4.12. Os serviços de assistência técnica preventiva e/ou corretiva serão prestados remotamente a todos os produtos fornecidos pela CONTRATADA, podendo ser realizados nas dependências da CONTRATANTE, desde que haja necessidade e prévia autorização pela CONTRATANTE ou a pedido desta.

4.13. A CONTRATADA deverá manter atualizados os equipamentos destinados à execução dos serviços, implementando as últimas versões estáveis, atualizações e correções de hardware e software recomendadas pelo fabricante, de modo a assegurar a plena integridade, segurança e o desempenho do ambiente em produção, de forma programada em acordo com a equipe de infraestrutura de produção do MPDFT.

4.14. A CONTRATADA será a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do Contrato;

4.15. A CONTRATADA deverá disponibilizar à CONTRATANTE serviço para abertura e acompanhamento de chamados que deverá estar acessível durante 24 horas por dia, 7 dias por semana, 365 dias por ano, sem ônus adicional para a CONTRATANTE, constituído de no mínimo:

4.15.1. Serviço de atendimento com discagem gratuita (0800) ou de custo local para telefone fixo (DDD 61);

4.15.2. E-mail;

4.15.3. Sítio Web com HTTPS como meio de comunicação de disponibilidade imediata, em língua portuguesa e/ou inglesa, que possibilite:

4.15.3.1. Gerar relatórios administrativos customizáveis de modo a permitir a seleção de períodos de abrangência, em forma de textos e gráficos, com possibilidade de exportar para HTML ou PDF ou CSV.

4.15.3.2. Visualizar informações relacionadas aos chamados técnicos: data e hora de abertura da solicitação; Identificação do solicitante, código de identificação da solicitação, descrição da solicitação, andamento da

solicitação (*worklog*), data e hora de fechamento da solicitação;

4.16. Serão abertos chamados de severidade Alta ou Média para a realização da assistência técnica corretiva;

4.17. A CONTRATADA encaminhará mensagem de e-mail para os contatos definidos pela CONTRATANTE informando, no mínimo, o número do chamado, a severidade, a data e hora da solicitação, nome do SOLICITANTE, descrição detalhada da solicitação;

4.18. A CONTRATANTE terá acesso ao sistema Web da CONTRATADA para acompanhamento, consulta, histórico dos chamados abertos, independentes da sua forma de abertura;

4.19. A CONTRATADA somente poderá efetuar manutenção técnica que tenha previsão de indisponibilidade na solução e seus componentes após aprovação por parte da CONTRATANTE.

4.20. É vedado à CONTRATADA interromper o atendimento de um chamado até que, RECOLOCANDO EM PLENO ESTADO DE FUNCIONAMENTO, se chegue à solução definitiva. A CONTRATADA comunicará o fato à equipe técnica da CONTRATANTE e solicitará autorização para o fechamento do chamado;

4.21. A CONTRATANTE encaminhará à CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal de até 10 usuários que terão *login* e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados. Esses perfis serão criados a critério da CONTRATANTE e configurados pela CONTRATADA. Essa lista pode mudar durante o período de vigência do contrato;

4.22. Caberá à CONTRATADA gerenciar permanentemente durante toda a vigência do contrato, de forma proativa, toda a solução adquirida, garantindo os níveis de serviço acordados;

4.23. Caso seja necessária a instalação de equipamentos de administração da solução nas instalações do CONTRATANTE, a CONTRATADA deverá fornecer todos os recursos necessários para tanto. O CONTRATANTE ficará responsável apenas pelo fornecimento de alimentação elétrica e portas lógicas para as conexões;

4.24. O acesso aos equipamentos eventualmente hospedados no MPDFT dar-se-á por meio de VPNs via Internet, a serem implementadas pela CONTRATADA. De forma a possibilitar a administração remota, a CONTRATADA poderá optar por proceder a instalação e a manutenção de canal de comunicação direto com os equipamentos sob sua responsabilidade, devendo se responsabilizar e garantir total segurança para este acesso. Atuações locais, que necessitem de acesso físico direto ao ambiente e ao equipamento, deverão ser previamente comunicados e acordados com a equipe do MPDFT;

4.25. O CONTRATANTE possui link de internet que poderá ser utilizado para o

estabelecimento das VPNs mencionadas no item anterior;

4.26. A CONTRATADA deverá, por meio da administração remota, ser capaz de implementar políticas, regras, filtros ou quaisquer outros recursos e implementações lógicas, necessárias a manutenção do serviço em conformidade com o especificado. As solicitações de alterações e inclusões de novas políticas, regras e filtros efetuados pelo CONTRATANTE não serão limitadas e deverão ser implementadas, de acordo com o NMSE;

4.27. A CONTRATADA deverá criar contas de acesso privilegiado à administração dos serviços para a equipe técnica do CONTRATANTE, que permitam a execução de funções de administração da solução, em especial alterações e inclusões de novas políticas, regras e filtros. Todos os acessos à administração dos serviços, inclusive aqueles efetuados pela CONTRATADA, deverão ser autenticados, criptografados e registrados para posterior auditoria;

4.28. A instalação, remoção ou desligamento das funcionalidades dos equipamentos deverá, sempre que possível, ser realizada sem que outros componentes da rede local do CONTRATANTE necessitem de configuração adicional;

4.29. A CONTRATADA deverá desempenhar suas atividades por intermédio de pelo menos dois técnicos devidamente identificados, especializados e qualificados da seguinte forma: formação específica e oficial do fabricante para as atividades de instalação, configuração e suporte, envolvendo os componentes da solução, a ser comprovada com certificado e/ou declaração de curso(s) técnico(s), emitidos pelo fabricante dos mesmos ou empresa credenciada e qualificada para esta finalidade;

4.30. A CONTRATADA deverá enviar à CONTRATANTE a relação dos técnicos que devem ser autorizados a entrar nas dependências da CONTRATADA, juntamente com os documentos necessários para cadastro na segurança institucional do órgão. Para acesso à sala cofre é necessário cadastramento biométrico dos técnicos, que deverá ser agendado com a CONTRATANTE;

4.31. Caso a Equipe de Atendimento Técnico da CONTRATADA sofra alguma alteração em sua composição durante a vigência deste contrato, tal fato deve ser imediatamente informado ao gestor do contrato e à equipe técnica do MPDFT, incluindo as respectivas comprovações acerca dos requisitos de qualificação exigidos para esses profissionais e as informações necessárias para liberação do acesso dos técnicos às dependências do MPDFT, conforme itens anteriores;

4.32. Caso seja constatada a falta de conhecimento mínimo necessário para operação da solução por parte do prestador de serviço, a equipe técnica do MPDFT poderá solicitar sua substituição por técnico devidamente qualificado.

5. REQUISITOS DA CONTRATAÇÃO (ITENS 1, 2, 3 e 4)

5.1. DOCUMENTAÇÃO TÉCNICA

5.1.1. Deverá ser entregue pela CONTRATADA a "Documentação Técnica" (DT) de toda a solução implementada no ambiente da CONTRATANTE, composta de:

5.1.1.1. Plano de Implantação, contendo as configurações específicas dos equipamentos, arquiteturas e suas topologias e diagramas lógicos da solução;

5.1.1.2. Plano de Testes;

5.1.1.3. Plano de Transferência de Conhecimento;

5.1.2. Essa documentação fica sujeita à análise e à aprovação da equipe técnica da CONTRATANTE;

5.1.3. Toda a DT deverá ser entregue em mídia digital, devendo as topologias da solução serem entregues em formato a ser definido pela CONTRATANTE;

5.1.4. Essa documentação fica sujeita à análise e aprovação da equipe técnica da CONTRATANTE;

5.1.5. Toda a DT fornecida pela CONTRATADA referente às ferramentas e solução implantadas no ambiente da CONTRATANTE é de propriedade da CONTRATANTE.

5.1.6. Toda a DT fornecida pela CONTRATADA deverá estar em português do Brasil.

5.2. REUNIÃO DE ALINHAMENTO DE EXPECTATIVAS

5.2.1. Deverá ser realizada uma reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus Anexos, e esclarecer possíveis dúvidas acerca da infraestrutura de TI da CONTRATANTE;

5.2.2. Deverão participar dessa reunião, no mínimo, o Gestor do Contrato, o Fiscal Técnico do Contrato, o Preposto e membro da equipe técnica da CONTRATADA;

5.2.3. A reunião realizar-se-á na sede da CONTRATANTE em prazo especificado neste documento;

5.2.4. Na reunião de Alinhamento de Expectativas a CONTRATADA deverá apresentar:

5.2.4.1. Sugestão de conjunto de políticas, regras e filtros a serem configurados na solução de gerenciamento de acessos privilegiados;

5.2.4.2. As sugestões deverão ser apresentadas para discussão durante a reunião e as configurações definitivas devem ser apresentadas no Plano de Implantação.

5.2.5. Durante a implantação, o conjunto de políticas, regras e filtros de que trata o item anterior poderão ser alterados conforme a necessidade da CONTRATANTE.

5.3. CREDENCIAMENTO DOS COLABORADORES

5.3.1. Todos os profissionais que prestarem serviços relativos à solução devem ser credenciados junto ao MPDFT para que sejam autorizados a prestar serviços nas dependências do órgão.

5.3.2. A CONTRATADA deverá observar, rigorosamente, todas as normas, padrões e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do MPDFT.

5.3.3. Para acesso à sala cofre é necessário cadastramento biométrico dos técnicos, que deverá ser agendado com a CONTRATANTE.

5.3.4. Caberá à CONTRATADA comunicar ao MPDFT qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do MPDFT, porventura colocados à disposição para realização dos serviços contratados.

5.3.5. Deve ser mantido sigilo sobre todos os ativos de informações e de processos do MPDFT e da CONTRATADA que se refiram ao MPDFT.

5.3.6. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do MPDFT, sob pena de aplicação das sanções cabíveis.

5.3.7. A CONTRATADA deverá manter em caráter confidencial, as informações relativas à política de segurança adotada pelo MPDFT e as configurações de hardware e de Softwares decorrentes.

5.3.8. A CONTRATADA deverá manter em caráter confidencial, as informações relativas ao processo de instalação, configuração e adaptações de produtos e ferramentas.

5.3.9. A CONTRATADA deverá submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pelo MPDFT, durante o tempo de permanência nas dependências do órgão.

5.4. IMPLANTAÇÃO E HOMOLOGAÇÃO

5.4.1. A CONTRATADA deverá apresentar um Plano de Implantação que será avaliado e aprovado pela equipe técnica da CONTRATANTE;

5.4.2. O Plano de Implantação deverá conter a descrição de, no mínimo:

5.4.2.1. Atividades a serem desenvolvidas, incluindo testes, e seus respectivos cronogramas;

5.4.2.2. Políticas de configuração dos elementos da solução;

5.4.2.3. Topologia lógica para a solução;

5.4.2.4. Ações de *rollback*.

5.4.3. Todo o trabalho a ser realizado deve seguir o especificado no Plano de Implantação;

5.4.4. Para cada nova *release*, *build* ou funcionalidade, poderá ser solicitada uma nova implantação de qualquer funcionalidade presente na solução;

5.4.5. A CONTRATADA deverá realizar toda a instalação dos produtos, incluindo a configuração das ferramentas e os testes da solução, sob supervisão da CONTRATANTE;

5.4.6. Todas as atividades envolvidas na Implantação deverão ser acompanhadas pela equipe técnica da CONTRATANTE;

5.4.7. Todos os técnicos envolvidos na instalação e configuração devem possuir conhecimentos técnicos aprofundados nos produtos que ficarem sob sua responsabilidade de acordo com este termo de referência;

5.4.8. A CONTRATADA será responsável por dimensionar a solução a ser adotada na rede da CONTRATANTE atendendo minimamente os requisitos solicitados neste termo de referência. Esta solução estará sujeita à análise e aprovação da equipe técnica da CONTRATANTE;

5.4.9. A solução apresentada não pode causar impacto no funcionamento da rede (por exemplo, lentidão na rede local, degradação no desempenho das estações de trabalho e servidores, entre outros), devendo ser transparente ao usuário;

5.4.10. Caso o dimensionamento feito pela CONTRATADA não apresentar desempenho satisfatório, baseado nas recomendações do fabricante e conforme exposto no item anterior, a solução deverá ser redimensionada sem ônus adicional para a CONTRATANTE, mesmo que o redimensionamento envolva adição/substituição de hardware e software;

5.4.11. Junto com o Plano de Implantação, a CONTRATADA deverá apresentar um Plano de Testes à equipe técnica da CONTRATANTE para avaliação;

5.4.12. O Plano de Testes consiste num documento onde estão descritos todos os testes a serem realizados a fim de verificar todas as funcionalidades dos produtos oferecidos, descritas neste Termo;

5.4.13. O Plano de Testes deve ser apresentado em forma de tabela a fim de facilitar o acompanhamento por parte da CONTRATANTE;

5.4.14. Na tabela mencionada no item anterior, deve-se incluir os resultados esperados para cada teste realizado, conforme Modelo de Plano de Testes no Anexo II;

5.4.15. Os procedimentos descritos no Plano de Testes serão realizados pela CONTRATADA após a instalação e configuração dos produtos. Esses testes serão acompanhados pela equipe técnica da CONTRATANTE;

5.4.16. Caso seja detectado qualquer problema nos testes, em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização dessas correções, os testes serão reiniciados;

5.4.17. Se todos os testes forem realizados com sucesso, os produtos serão considerados implantados;

5.4.18. A CONTRATADA deverá fornecer todos os materiais necessários à instalação física, à configuração e ao perfeito funcionamento dos equipamentos, cabos elétricos e cabos lógicos, quando for o caso. Caberá à CONTRATANTE o provimento de alimentação elétrica e das portas lógicas para conexão à rede local;

5.4.19. Para a homologação da solução, será estabelecido pela CONTRATANTE um PFE - Período de Funcionamento Experimental, com duração definida conforme este Termo de Referência, para testar o perfeito funcionamento dos produtos, verificar suas funcionalidades, analisando sua aderência às especificações deste Edital e seus Anexos, bem como à Proposta da CONTRATADA, e a sua compatibilidade com a estrutura já existente na CONTRATANTE;

5.4.20. O PFE somente poderá ser iniciado após a conclusão da implantação e deve respeitar o prazo máximo definido neste Termo de Referência.

5.4.21. Pelo menos um técnico da CONTRATADA deverá acompanhar presencialmente o decorrer do PFE.

5.4.22. Durante o PFE, não deve ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades dos produtos fornecidos;

5.4.22.1. Caso haja qualquer falha ou interrupção em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização destas correções, o PFE será reiniciado.

5.4.22.2. Caso não haja qualquer falha ou interrupção em qualquer uma das funcionalidades, a solução será considerada homologada.

5.4.23. Os produtos funcionarão de acordo com as recomendações do fabricante, levando-se em consideração que todas as funcionalidades requeridas neste Termo de Referência estarão habilitadas simultaneamente;

5.4.24. A emissão do Termo de Homologação está vinculada à homologação, entrega da Documentação Técnica - DT e a realização da Transferência de Conhecimento, conforme mencionado neste Termo de Referência;

5.4.25. As etapas de implantação e PFE deverão ser contíguas, não havendo interstícios entre elas.

6. NÍVEIS MÍNIMOS DE SERVIÇO EXIGIDOS (NMSE)

6.1. Na abertura de chamado técnico de suporte, os chamados deverão ser categorizados de acordo com a severidade e atendidos nos devidos prazos.

Grau de severidade	Definição	Tempo de resposta
ALTA	Esse nível de severidade é aplicado para resolução de problemas, como a indisponibilidade da solução ou em qualquer funcionalidade que a compõe.	Prazo de solução: **4 horas** após abertura do chamado
MÉDIA	Esse nível de severidade é aplicado para solicitações de alteração de configurações, qualquer outra ação, de natureza ainda corretiva, que não se encaixe como resolução de problemas.	Prazo de solução: **8 horas** após abertura do chamado
BAIXA	Esse nível de severidade é aplicado para: solicitação de manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos; ou atualização dos produtos que compõem a solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados.	Prazo de solução**: 72 horas** após abertura do chamado

6.2. Fica também estabelecido que haverá glosa sobre o valor mensal da solução, por hora ou fração de hora em atraso no atendimento de chamados, conforme a seguinte fórmula:

$G = ((H_a * F_c) + (H_m * F_c) + (H_b * F_c)) * 4$, onde:

G = Percentual de glosa no mês;

H_a = Quantidade de horas em atraso de chamados de severidade ALTA;

H_m = Quantidade de horas em atraso de chamados de severidade MÉDIA;

H_b = Quantidade de horas em atraso de chamados de severidade BAIXA;

F_c = Fator de correção de severidade, sendo:

0,5 para severidade ALTA;

0,25 para severidade MÉDIA; e

0,125 para severidade BAIXA;

6.3. O percentual de glosa no mês, resultante da fórmula do item anterior, ficará limitado a 50% do valor mensal do contrato.

6.4. Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação de glosas previstas, poderá ser aberto processo específico pela CONTRATANTE para apuração de possível aplicação de penalidade.

ANEXO II – Modelo de Comprovação Ponto a Ponto

Tabela – comprovação de atendimento ponto a ponto

Código do item da especificação técnica do Termo de referência	Especificação Técnica	Referência na documentação oficial	Transcrição
1.x.x	AES com chaves de 256 bits;	Datasheetpág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
1.x.x	Permitir a criação de conjuntos de permissões automáticas de acordo com ativos descobertos;	InstalationGuide, pág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
1.x.x	Incluir o suporte para gerenciamento de sessões RDP e SSH, sem depender de integrações com ferramentas de terceiros;	Productguide, pág.xx, parágrafo(s) yy	"texto do documento oficial referenciado"
...	...	...	...
...	...	...	...

_____(nome e assinatura)_____

Nome completo, telefone e e-mail

ANEXO III – Modelo de Plano de Testes

Tabela – Modelo de Plano de Testes

Descrição do Teste	Resultado Esperado	Resultado Obtido
1. Validar geração de Logs de transferência de mensagens;	Visualizar os logs dentro da interface de gerência do equipamento	OK / FALHA
2. Configurar envio de logs para centralizador de logs;	Recebimento de logs pelo centralizador de logs	OK / FALHA
3. Integrar-se com servidores de autenticação Microsoft Active Directory para verificação de destinatários validos;	Listar caixas postais dos usuários	OK / FALHA
4. Validar implementação do modo cluster	Nós do cluster com comunicação de controle efetiva	OK / FALHA

_____(nome e assinatura)_____

Nome completo, telefone e e-mail

ANEXO IV – Modelo de Proposta de Preços

Tabela – Modelo de Proposta de Preços

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	1	Solução de gerenciamento de acessos privilegiados (Privileged Access Management – PAM), incluindo garantia do fabricante e atualização de versão pelo período de 5 anos.	Unidade	1	(numerais)	(numerais)
	2	Serviços de implantação, instalação e configuração da solução contratada	Serviço	1	(numerais)	(numerais)
	3	Transferência de conhecimento	Serviço	1	(numerais)	(numerais)
	4	Serviço de suporte técnico	Mês	36	(numerais)	(numerais)
VALOR TOTAL GLOBAL						**(numerais)**

_____(nome e assinatura)_____

Nome completo, telefone e e-mail

Assinado por:

DANIEL GUIMARÃES PENA - SESEG/STI em 10/09/2021.
MICHELLE DE CASTRO CARNEIRO - SECONSTI/STI em 10/09/2021.
PAULO CARVALHO ESPÍNDOLA FILHO - SESEG/STI em 10/09/2021.
PAULO LUIZ ALMEIDA DOS REIS - SECONSTI/STI em 10/09/2021.
.