

ANEXO - A

CADERNO DE ESPECIFICAÇÕES TÉCNICAS

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE
1	Solução de Suporte remoto protegido, integrado a gerenciador seguro de credenciais, aplicado às estações de trabalho de TIC.	Licenças/Usuários	Deverá ser observado o item do TR 1.2. Estimativas de consumo individualizadas, do órgão gerenciador e órgão(s) e entidade(s) participante(s)
2	Solução de acesso remoto seguro voltada para ambientes com requisitos elevados de segurança, aplicável a dispositivos com repositório de contas privilegiadas, com capacidade de usuários simultâneos compatível com a demanda estimada no Termo de Referência.	Licenças/Dispositivos	
3	Serviço de suporte técnico com operação assistida.	Mês	
4	Treinamento (Turma de 10 alunos).	Turma	
As referências tecnológicas constantes deste Anexo, quando existentes, possuem caráter meramente exemplificativo, admitindo-se soluções equivalentes ou superiores, desde que atendidos integralmente os requisitos funcionais, operacionais e de segurança estabelecidos.			

1. Solução de Suporte remoto protegido, integrado a gerenciador seguro de credenciais, aplicado às estações de trabalho de TIC

1.1. O licenciamento deverá contemplar o quantitativo previsto no item 1.2 do Termo de Referência, observadas as estimativas individualizadas do órgão gerenciador e dos partícipes, permitindo atendimento simultâneo compatível com a quantidade de estações de trabalho indicada no item 7 do ETP.

1.2. A solução deve utilizar mecanismos criptográficos robustos para proteção de dados em trânsito e em repouso, preferencialmente com módulos criptográficos validados conforme FIPS 140-2, FIPS 140-3 ou padrão equivalente reconhecido, garantindo proteção contra acessos não autorizados.

a) A solução deve integrar-se a sistemas existentes sem comprometer a segurança.

1.3. A solução deve permitir o início da sessão remota de suporte técnico a partir de console centralizado pelo técnico de TI (interface web ou cliente instalado), ou, alternativamente, mediante solicitação do usuário final registrada por meio de integração com sistema de chamados (ITSM), portal web autenticado, ou identificador

único de sessão emitido pela plataforma.

1.4. A solução deve evitar o uso de protocolos de comunicação legados necessários para acesso, dando preferência a protocolos totalmente criptografados.

1.5. A solução deve permitir o início da sessão a partir de cliente instalado na estação do técnico, interface web autenticada, ou, alternativamente, fluxo iniciado a partir do registro do chamado no sistema ITSM integrado, com seleção do recurso, do administrador responsável ou da categoria do atendimento.

1.6. A solução deve permitir o acesso remoto às estações de trabalho sem necessidade de instalação prévia obrigatória de componentes cliente persistentes, podendo o componente ser baixado e executado no momento da sessão, ou, alternativamente, utilizar agente leve previamente distribuído nas estações gerenciadas, com remoção/desativação controlada conforme política, preservando a auditoria e o registro completo da sessão.

1.7. Permitir elevar privilégios do cliente no momento da sessão para execução de tarefas administrativas, sem perder a conexão.

1.8. Possuir a funcionalidade de provedor de elevação de acesso, caso o administrador precise elevar os privilégios da sessão e não possua a credencial necessária, com integração ao gerenciador seguro de credenciais.

1.9. Solução deve suportar a injeção automática de senhas, permitindo que os usuários autenticuem ou elevem privilégios para desktops e sistemas remotos, sem revelar credenciais e senhas de texto simples. Permitindo que os usuários selecionem a credencial a ser utilizada a partir de uma lista de credenciais que têm privilégios no sistema.

1.10. A solução deve permitir iniciar sessão com acesso integral ao desktop remoto, ou, alternativamente, com acesso restrito a aplicações específicas publicadas pela plataforma (Remote Applications), conforme política definida.

1.11. Permitir iniciar sessão com usuário fora da rede interna.

1.12. A solução deve permitir a execução de comandos e scripts em sessões shell (SSH/CLI), com possibilidade de catálogo de comandos pré-aprovados centralizados na plataforma e disponibilização durante a sessão conforme política, sem exposição direta ao usuário final.

1.13. Permitir transferência de arquivos em uma sessão através de interface arrastar e

colar.

1.14. A solução deve permitir consulta a informações estruturadas dos ativos gerenciados (inventário), contemplando, no mínimo, identificador, sistema operacional, endereço IP, estado da conexão e metadados de inventário disponíveis na plataforma, conforme perfil de acesso autorizado.

1.15. A solução deve permitir comunicação textual entre os administradores envolvidos na sessão privilegiada (operador, supervisor, auditor) nativamente; e, quando aplicável, com o usuário final solicitante por meio de integração com sistema de chamados (ITSM).

1.16. A solução deve permitir que os administradores definam mensagens padronizadas que os representantes podem usar durante uma sessão.

1.17. A solução deve permitir a reinicialização do dispositivo remoto durante a sessão administrativa, com possibilidade de retomada da conexão após o reinício do sistema, mediante reabertura controlada da sessão pela plataforma, conforme política definida.

1.18. Permitir iniciar sessões administrativas por SSH, admitindo-se Telnet apenas para ativos legados formalmente identificados pela Contratante, desde que o acesso ocorra por mecanismo seguro de proxy, rede segregada ou túnel controlado, com auditoria, gravação e autorização específica.

1.19. A solução deve permitir personalização visual do portal externo de acesso (logotipo, identidade visual e mensagens informativas), com vistas ao alinhamento à identidade corporativa da Contratante.

1.20. Configuração de balanceamento de carga de trabalho, para automaticamente direcionar sessões novas para atendentes menos ocupados e de acordo com a experiência/especialidade de cada um.

1.21. Permitir que a sessão seja iniciada somente com chat.

1.22. Mostrar para o usuário em qual posição está na fila quando utilizar a função de iniciar sessão com chat.

1.23. Permitir que o atendente possa mostrar a própria tela ao usuário, revertendo o compartilhamento de tela.

1.24. Permitir desenhar e indicar com ponteiro visual na tela do usuário.

1.25. Permitir visualizar todas as telas de um cliente com mais de um monitor habilitado.

1.26. Permitir que o atendente bloqueie o mouse e teclado do usuário, e o usuário deve receber mensagens de como readquirir o controle da sessão.

1.27. Permitir, quando aplicável ao ambiente tecnológico da CONTRATANTE e compatível com os recursos nativamente disponíveis nos equipamentos administrados, integração ou suporte a mecanismos de gerenciamento remoto em nível inferior ao sistema operacional (out-of-band management), possibilitando acesso administrativo independentemente do estado do sistema operacional ou de energia do dispositivo.

1.28. Permitir que cada atendente trabalhe em múltiplas sessões ao mesmo tempo, independentemente da plataforma dos clientes atendidos.

1.29. A solução deve suportar conexões onde o usuário final possua vários monitores.

1.30. A solução deve permitir que os representantes transmitam sua tela para vários participantes, como um modo de apresentação.

1.31. Permitir estabelecer perfis de líder de equipe e gerente de equipe.

1.32. Possibilitar líder ou gerente de equipe visualizar um dashboard para monitorar e controlar as sessões da equipe.

1.33. Possibilitar líder ou gerente de equipe visualizar a tela de um atendente membro da equipe durante o atendimento de uma sessão.

1.34. Possibilitar pesquisa de satisfação com o cliente e com o atendente após finalizar sessão de suporte.

1.35. Permitir compartilhar a sessão com um ou mais representantes ou outra equipe, ou até mesmo de um usuário externo.

1.36. Permitir envio de convite para representante externo participar de uma sessão.

1.37. A solução deve permitir o compartilhamento ou a delegação de sessão privilegiada entre administradores autorizados ou equipes, com manutenção do registro de auditoria correspondente e identificação inequívoca da identidade ativa em cada momento.

1.38. Permitir chat entre os atendentes conectados.

1.39. A solução deve permitir o acesso a vários tipos de Sistemas Operacionais, com ou sem agentes, incluindo no mínimo o suporte aos seguintes:

- a) Sistemas operacionais Windows;
- b) Sistemas operacionais Mac OS;
- c) Sistemas operacionais Linux;
- d) Dispositivos móveis;
- e) Apple Ios;
- f) Android;

1.40. A solução deve disponibilizar ao usuário múltiplas formas de acesso a console da solução, incluindo:

- a) Uma console instalada diretamente no Sistema Operacional do cliente, que deve suportar Sistemas Operacionais Windows 64 Bit, Sistemas Operacionais Mac e também Sistemas operacionais Linux 64Bit;
- b) Uma console de acesso baseado em web que usa HTML5, ou seja, sem necessidade de nenhum plug-in ou agente especial para fornecer o acesso. Esta console Web deve eliminar o requisito de ter que baixar e instalar um cliente de acesso;
- c) Uma console de acesso para iOS que deve estar disponível para download gratuito na Apple App Store;
- d) Uma console de acesso para Android que deve estar disponível para download gratuito no Google Play;

1.41. Permitir criação de políticas para grupos de usuários para controlar acessos e permissões.

1.42. Armazenar em log no sistema informações das sessões (nome e máquina do usuário e do atendente, chat, transferências de arquivos, informações do sistema, e o vídeo do atendimento).

1.43. A gravação da sessão deve permitir reprodução íntegra para fins de auditoria, com identificação clara da identidade do administrador responsável e do ativo acessado, ao longo de toda a duração da sessão.

1.44. Relatórios das conversas via chat.

1.45. Permitir ao usuário ver ou baixar uma cópia do chat depois de terminada a sessão.

1.46. Relatórios detalhados das sessões de suporte.

1.47. Permitir que os representantes possam se autenticar e autorizar em diretórios LDAP, utilizando os grupos do LDAP para autorização.

1.48. Restringir acesso a console de atendimento para IPs específicos.

1.49. A fim de adicionar uma camada adicional na segurança da autenticação de usuários, a solução deve suportar duplo fator de autenticação, suportando no mínimo:

- a) Integração com soluções de autenticação de dois fatores via RADIUS;
- b) A solução deve suportar autenticação multifator baseada em senha única temporária (TOTP), compatível com aplicativos autenticadores aderentes a padrões

de mercado;

c) Deve ser possível a utilização de SmartCard para autenticação do representante de suporte;

d) A solução deve suportar autenticação biométrica compatível com o dispositivo;

e) Possuir API aberta para construção de outras integrações;

1.50. A solução deverá possuir integração com ferramentas de ITSM e gerenciamento de chamados, por meio de conectores nativos, APIs documentadas, webhooks ou mecanismos equivalentes, possibilitando abertura, acompanhamento e correlação de incidentes e requisições.

1.51. Ser compatível com firewall e ambientes de DMZ para permitir acesso a usuários e de atendentes pela internet.

1.52. Permitir que os servidores/appliance trabalhem em alta disponibilidade.

1.53. Possuir componente Proxy para acesso a equipamentos de redes externas.

1.54. Deve possibilitar a gravação automática das sessões de compartilhamento de tela e linha de comando, sendo que na gravação do compartilhamento de tela, a solução deve possibilitar tornar dados de um usuário ou máquina específicos anônimos nas gravações de sessão, no caso de uma determinação de auditoria ou compliance.

1.55. Deve permitir que o representante de suporte reinicialize o dispositivo remoto e após a reinicialização, a sessão seja restabelecida automaticamente sem a necessidade de iniciar outra sessão.

1.56. Deve suportar comunicação segura e eficiente para sessões de compartilhamento de tela, transferência de arquivos ou shell remoto, podendo utilizar arquitetura peer-to-peer, proxy, relay intermediário ou mecanismo equivalente, preservando desempenho, segurança e rastreabilidade das sessões.

1.57. Deve permitir iniciar sessões remotas a dispositivos não assistidos, onde não existam usuários solicitando suporte.

1.58. Deve possibilitar configurar, que, ao iniciar a sessão, o mouse e o teclado iniciem de forma restrita ao representante de suporte.

1.59. A solução deverá permitir a execução remota de atividades administrativas em sistemas Windows, incluindo, quando suportado pela solução ofertada, operações relacionadas ao registro do sistema, sem obrigatoriedade de compartilhamento integral da tela.

1.60. Solução deve forçar que conteúdo não confiável não deve poder fazer modificações no sistema operacional, no registro e nos aplicativos instalados.

1.61. A solução deve permitir que os usuários compartilhem sessões de acesso com outros usuários do sistema, permitindo que os administradores colaborem em uma mesma sessão. Esta colaboração deve ser possível com usuários internos e também com usuários externos através de convite.

2. Solução de acesso remoto seguro voltada para ambientes com requisitos elevados de segurança, aplicável a dispositivos com repositório de contas privilegiadas, com capacidade de usuários simultâneos compatível com a demanda estimada no Termo de Referência.

2.1. O licenciamento da solução deverá observar o quantitativo estimado no item 1.2 do Termo de Referência, contemplando órgão gerenciador e partícipes, permitindo o acesso simultâneo compatível com a demanda operacional prevista, sem limitação indevida ao uso regular do ambiente pelos usuários autorizados, independentemente da quantidade de usuários privilegiados cadastrados, observadas as métricas comerciais da proposta vencedora.

2.2. A solução deve evitar o uso de protocolos de comunicação legados necessários para acesso, dando preferência a um protocolo totalmente criptografado, suportando protocolo criptográfico seguro, no mínimo TLS 1.2 ou superior.

2.3. A solução deve suportar seu funcionamento dentro de redes que não estão diretamente conectadas à internet.

2.4. A solução deve suportar o acesso desacompanhado, sem necessidade de permissão prévia a servidores de rede físicos e virtuais e dispositivos de rede.

2.5. A solução deve possibilitar acesso seguro a dispositivos de rede, como roteadores, switches, firewalls e outros ativos administrativos, preferencialmente por SSH. O uso de Telnet somente será admitido para ativos legados que não suportem protocolo seguro, mediante autorização formal da Contratante, controle por política, auditoria integral da sessão e adoção de mecanismo que evite exposição direta do protocolo em redes inseguras.

2.6. A solução deve utilizar mecanismos criptográficos robustos para proteção de dados em trânsito e em repouso, preferencialmente com módulos criptográficos validados conforme FIPS 140-2, FIPS 140-3 ou padrão equivalente reconhecido, garantindo proteção contra acessos não autorizados.

- a) A solução deve integrar-se, sem comprometer a segurança, aos sistemas corporativos requeridos pelo ambiente, incluindo quando aplicáveis diretórios corporativos, provedores de identidade, mecanismos de autenticação multifator, ferramentas de SIEM, ITSM.

2.7. A solução deve disponibilizar ao usuário múltiplas formas de acesso a console da solução, incluindo:

2.7.1. A solução deve disponibilizar ao usuário múltiplas formas de acesso à console administrativa, podendo ser um cliente instalado diretamente no Sistema Operacional do cliente ou interface web segura por navegador.

2.8. A solução deve oferecer suporte a provedores de identidade externos para autenticação, suportando a autenticar usuários em no mínimo servidores LDAP, Active Directory, RADIUS ou Kerberos existentes, bem como para atribuir privilégios com base na hierarquia já existente e nas configurações de grupo já especificadas nos respectivos servidores.

2.9. A solução deve possuir, de forma nativa ou por módulo oficial integrado, interface para armazenamento seguro de credenciais, segredos, chaves e informações sensíveis associadas a contas e acessos privilegiados.

2.10. A solução deve garantir requisitos de segurança na guarda de credenciais, incluindo criptografia no tráfego de informações, suportando, no mínimo, TLS 1.2;

2.11. Quando aplicável ao ambiente da Contratante, a solução deverá possuir recursos para gerenciamento seguro de credenciais utilizadas por aplicações, reduzindo o uso de credenciais estáticas em códigos-fonte, scripts ou arquivos de configuração.

2.11.1. Atualização automática de contas no banco de dados de senhas;

2.11.2. Inscrição automática de sistemas alvo sem aguardar por atualizações dinâmicas;

2.11.3. Configurações de segurança que garantam o acesso apenas por aplicações permitidas, suportando no mínimo o endereço de origem das requisições, nome de usuário, autenticação por certificados e/ou caminho da aplicação.

2.12. A fim de adicionar uma camada adicional na segurança da autenticação de usuários, a solução deve suportar duplo fator de autenticação, suportando no mínimo:

- a) Integração com soluções de autenticação de dois fatores via RADIUS.
- b) A solução deve suportar autenticação multifator baseada em senha única temporária (TOTP), compatível com aplicativos autenticadores aderentes a padrões de mercado.
- c) A solução deve suportar autenticação biométrica compatível com o dispositivo.

- d) A solução deve suportar padrão de autenticação FIDO2.
- e) A solução deve suportar logon único (SSO), comunicando-se com um provedor de identidade usando SAML 2.0.
- f) A solução deve suportar a utilização de certificados digitais válidos, emitidos por autoridade certificadora reconhecida publicamente ou por infraestrutura de certificação interna da Contratante, conforme a arquitetura definida para implantação.

2.13. A solução deve possuir políticas a serem usadas para controlar quando os ativos podem ser acessados, suportando no mínimo:

- a) Programação para definir quando os ativos sob esta política podem ser acessados. A política deve permitir a definição do fuso horário a ser utilizado no agendamento, permitindo uma ou mais opções de agendamento do acesso. Definindo o dia e hora de início e o dia e hora de término.
- b) Para certos grupos de usuários, a solução deve permitir forçar o encerramento da sessão. Forçando a sessão a se desconectar no horário final agendado. Nesse caso, o usuário deve receber notificações antes de ser desconectado.
- c) Notificar destinatários quando uma sessão é iniciada. Suportando no mínimo
- d) uma notificação por e-mail a destinatários designados sempre que uma sessão é iniciada com qualquer ativo.
- e) Notificar destinatários quando uma sessão é terminada. Suportando no mínimo uma notificação por e-mail a destinatários designados sempre que uma sessão é encerrada com qualquer ativo.
- f) Exigir aprovação antes do início de uma sessão, suportando no mínimo uma notificação por e-mail de aprovação enviado aos destinatários designados sempre que uma tentativa de sessão com qualquer ativo. Solicitando que o usuário insira um motivo da solicitação, a hora e a duração da solicitação.

2.14. A solução deve manter uma gravação completa e à prova de falsificação de todas as atividades da área de trabalho e do shell de comando.

2.15. A solução deve manter um registro completo de todas as atividades executadas durante a sessão executada pelos usuários.

2.16. A solução deve permitir o monitoramento ao vivo das sessões de acesso, e também deve permitir que os administradores encerrem sessões em andamento se

necessário.

2.17. A solução deve permitir a configuração de permissões granulares, oferecendo a capacidade de controlar e delegar permissões por usuários e por função.

2.18. A solução deve permitir definição de políticas de restrição, controle ou supervisão da execução de aplicações durante sessões privilegiadas, de forma nativa ou por integração com mecanismos complementares de segurança do ambiente.

2.19. A solução deve permitir a elevação de privilégios para aplicações que requeiram User Account Control (UAC) e para aplicativos pertencentes a proprietários confiáveis (System, Administradores ou Trusted Installer).

2.20. Permitir que as opções de “run as” e “executar como Administrador” sejam omitidas ao usuário final, permitindo a elevação sobre demandas através de uma mensagem customizada oferecida pela ferramenta;

2.21. A fim de proteger contra erros comuns do usuário durante as sessões SSH, solução deve suportar filtro de comandos, para bloquear alguns comandos e permitir que outros, em um esforço para evitar que o usuário inadvertidamente use um comando que pode causar resultados indesejáveis.

2.22. Ao acessar um ativo baseado em Windows, a injeção de credenciais deve ser suportada na tela de login, bem como a ação especial "Executar como", além de permitir a elevação sobre demanda de aplicativos classificados por regra, isso é, permitir que a opção padrão de “executar como administrador” seja automaticamente elevada a aplicativos previamente configurados, sem qualquer interação ou autenticação necessária ao usuário final.

2.23. Ao acessar um ativo baseado em Linux, usando injeção de credenciais, sendo que, para as credenciais que serão injetadas nos ativos, sejam eles Windows ou Linux, as mesmas deverão ser descobertas pela solução de forma automatizada, com a descrição inclusive se as credenciais descobertas são privilegiadas ou não, sendo que as credenciais descobertas poderão ser randomizadas para aumentar o nível de segurança do ambiente tecnológico.

2.24. A solução deve suportar acesso remoto seguro a ativos privilegiados por meio de interface web segura ou cliente instalado, com gerenciamento centralizado das conexões, políticas e registros de auditoria. Suportando os seguintes modos:

a) Através de clientes instalados, que permite o acesso a qualquer sistema

Windows, Mac ou Linux. Tendo total Gerência e relatórios centralizados de todos os clientes implantados.

b) A solução deve suportar acesso remoto seguro por mecanismos de proxy/jump seguro, sem exposição direta dos ativos e credenciais ao usuário.

c) A solução deve suportar acesso remoto seguro a ativos localizados em redes segmentadas ou com conectividade restrita, preservando auditoria, rastreabilidade e segurança da sessão.

d) A solução deve suportar acesso remoto via RDP com auditoria, gravação, monitoramento e aplicação de políticas de acesso privilegiado.

e) Acesso a dispositivos de rede habilitados para SSH e, excepcionalmente, Telnet para ativos legados formalmente autorizados.

f) Caso necessário ao ambiente, a solução poderá suportar protocolos adicionais de acesso remoto, desde que preservadas as capacidades de auditoria, gravação e controle de acesso.

g) A solução deve permitir acesso seguro e auditável a interfaces web administrativas, quando aplicável ao ambiente, sem exposição direta de credenciais privilegiadas.

h) A solução deve suportar, quando requerido, extensão segura de conectividade para protocolos administrativos específicos, preservando auditoria, rastreabilidade e controle de acesso.

2.25. A solução deve permitir o monitoramento em tempo real das sessões de acesso feitas a ativos publicados na ferramenta.

2.26. A solução deve permitir configuração de tempos limites de sessão ociosos, onde seja possível definir o período de tempo em qual um usuário que está inativo seja desconectado.

2.27. A solução deve permitir a correlação completa entre a identidade autenticada, a credencial utilizada, o ativo acessado, a sessão iniciada e as ações executadas, garantindo rastreabilidade fim a fim para auditoria e investigação.

2.28. A solução deve permitir transferência de arquivos entre o dispositivo local e o ativo remoto de forma auditável, controlada por política e associada à sessão privilegiada.

2.29. Em caso de colaboração de administradores em uma mesma sessão, a solução deve oferecer mecanismo de comunicação síncrona entre os administradores

envolvidos, podendo ser provido pela própria console de sessão ou por integração com ferramenta corporativa de comunicação institucional (Microsoft Teams ou equivalente), desde que o canal de comunicação esteja correlacionado à sessão privilegiada para fins de auditoria e rastreabilidade.

2.30. A solução deverá suportar recursos de análise comportamental aplicados aos acessos privilegiados e sessões administrativas, de forma nativa ou mediante integração com ferramentas especializadas de monitoramento, SIEM ou analytics.

2.31. A solução deve permitir a associação dos eventos comportamentais à identidade do usuário, credencial utilizada, ativo acessado e sessão correspondente, para fins de auditoria e investigação.

2.32. A solução deve permitir consulta remota a informações básicas do ativo, como sistema operacional, nome, endereço IP e estado da conexão, quando aplicável.

2.33. A solução deve oferecer aos representantes a capacidade de executar tarefas do sistema fora do compartilhamento de tela, com por exemplo reiniciar um serviço em servidores com sistema operacional Windows.

2.34. A solução deve oferecer a opção de prover acesso a linha de comandos dos servidores sem a necessidade de compartilhamento de tela, permitindo aos administradores a execução de comandos remotos via conexões lentas de internet.

2.35. Caso a solução ofereça automações ou execução assistida de comandos/scripts, tais funções devem ser auditáveis e controladas por perfil e política.

2.36. A solução deve suportar transferência auditável de arquivos entre dispositivo local e ativo remoto, podendo, opcionalmente, suportar fluxos adicionais entre ativos remotos.

2.37. A solução deve permitir a transferência de arquivos por meio de drag-and-drop ou suportar outros métodos para transferências de arquivos.

2.38. Caso requerido pelo ambiente, a solução poderá suportar funções adicionais de administração remota em ativos Windows, desde que auditáveis e controladas por política.

2.39. A solução deve permitir que o Administrador mude o portal externo com a marca corporativa, isto é, os administradores podem alterar a imagem de logotipo para exibição em páginas da Web voltadas para o público. Permitindo que os usuários externos verifiquem que estão no site de sua organização, além de aprimorar o portal

de acesso com a marca da organização.

2.40. A solução deve permitir organização administrativa de usuários e grupos, com delegação de papéis, segregação de funções e supervisão compatível com as políticas de acesso privilegiado.

2.41. A solução deve disponibilizar relatórios detalhados das sessões privilegiadas, contendo informações de acesso, duração, gravações, comandos executados e ativos envolvidos.

2.42. A solução deve disponibilizar trilha detalhada das atividades realizadas durante a sessão, incluindo comandos, arquivos transferidos e eventos relevantes de auditoria.

2.43. A solução deve conter também outras informações da sessão que incluem a duração da sessão, endereços IP locais e remotos e informações do sistema remoto.

2.44. A solução deve permitir a anonimização de dados sensíveis ou mecanismos equivalentes de proteção das evidências de auditoria, incluindo no mínimo controle de acesso granular, segregação por perfis/grupos e restrição de visualização de registros, relatórios e gravações.

2.45. A solução deve permitir visualização das evidências de auditoria compatíveis com o modo de acesso utilizado, incluindo gravações quando aplicável.

2.46. Caso o usuário utilize somente o prompt de comando do sistema, deve ser possível visualizar gravações e/ou transcrições de texto de todos os comandos executados durante a sessão.

2.47. A solução deve também conter relatórios resumidos que fornecem uma visão geral da atividade ao longo do tempo por usuário. Contendo informações como: O número total de sessões executadas, o número médio de sessões por dia da semana e a duração média das sessões.

2.48. A solução deve disponibilizar relatórios administrativos e operacionais sobre o uso da plataforma, contendo no mínimo informações sobre usuários, grupos, ativos acessados, sessões realizadas, duração, eventos relevantes de auditoria e evidências associadas, conforme perfil de acesso autorizado.

2.49. A solução deve ser capaz de integrar-se com ferramentas de SIEM.

2.50. Descrição da Garantia da solução de proteção de dispositivos:

- a) A CONTRATADA deverá fornecer suporte direto do fabricante da solução durante toda a vigência contratual para atualizações de versão e acionamento em nível de

resolução de problemas pelo próprio fabricante se necessário, além do nível de suporte que deverá ser prestado pela CONTRATADA em conjunto.

3. SERVIÇOS DE SUPORTE TÉCNICO COM OPERAÇÃO ASSISTIDA

3.1. O serviço de suporte técnico com operação assistida e transferência de conhecimento para a solução, será mensal e deverá ser executado durante toda vigência contratual.

3.2. A CONTRATADA deverá fornecer suporte direto do fabricante da solução durante toda a vigência contratual para atualizações de versão e acionamento em nível de resolução de problemas pelo próprio fabricante se necessário, além do nível de suporte que deverá ser prestado pela CONTRATADA em conjunto, conforme previsto neste Termo de Referência seus Apêndices.

3.3. Os atendimentos deverão ser do tipo telefônico e/ou internet 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, e deverá ser realizado por profissionais especializados, sendo necessário cobrir todo e qualquer defeito ou demanda apresentada.

3.4. Os serviços de suporte e manutenção consistem em atendimentos a dúvidas técnicas quanto ao uso do ambiente e de eventuais problemas identificados, diagnósticos de problemas técnicos e análises de tendências associadas a solução e seus componentes.

3.5. As atividades de suporte técnico serão realizadas, a critério do Órgão Contratante, a partir da assinatura do Contrato e durante toda sua vigência contratual.

3.6. Não estão contemplados problemas relacionados a hardware, uma vez que os recursos físicos serão de responsabilidade do Órgão Contratante.

3.7. O suporte técnico com operação assistida poderá ser utilizado para melhoria das configurações do ambiente, continuidade do processo de implantação e integração com os dispositivos do Órgão Contratante, além do desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:

- a) Orientação sobre acesso, o uso, a configuração, a instalação da solução e a integração com os dispositivos do Órgão Contratante, contando com acesso ao conhecimento privilegiado de recursos da CONTRATADA e quando necessário do

FABRICANTE da solução.

- b) Orientação quanto às melhores práticas para implementação e integração da solução no ambiente do Órgão Contratante.
- c) Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões da solução e seu impacto no gerenciamento dos acessos lógicos privilegiados no ambiente do Órgão Contratante.
- d) Análise técnica qualificada nas análises e prevenções de vulnerabilidades encontradas e passíveis de serem exploradas na solução de gerenciamento de acesso lógico privilegiado.
- e) Aplicação de melhores práticas para implementação do gerenciamento de acesso lógico privilegiado.
- f) Realização de estudos e configuração do ambiente e implementação das integrações necessárias, instáveis ou com comportamento errático caso aconteçam.
- g) Realização de atividades de operação assistida envolvendo profissionais capacitados para operar de forma assistida o funcionamento da solução de forma remota durante o horário de funcionamento do Ministério, bem como monitorar seu uso, realização de Health checks (exames de saúde do ambiente), realização de manutenções, criação e adequação de novos acessos remotos, revisão de acessos antigos, geração de relatórios de utilização, adequações e sugestões de configurações, operação e suporte da solução de acordo com a necessidade do Ministério.
- h) Realização de estudos para melhoria dos acessos lógicos do ambiente atual do Órgão Contratante.
- i) Implementação de novas integrações que não tenham ainda sido efetivadas ou sejam necessárias.
- j) Identificação de melhorias e respectivo tratamento (melhoria de parametrização).
- k) Parametrização da solução, de acordo com as regras e políticas de acessos lógicos remotos e privilegiados definidos pelo Órgão Contratante.
- l) Apoio na elaboração e adequação de relatórios executivos, gerenciais, de auditoria e operacionais quando necessário.
- m) Suporte avançado para estratégia e planejamento no gerenciamento de

acessos lógicos por meio da solução ao ambiente do Órgão Contratante.

n) Avaliação e comparação de novas funcionalidades de forma remota e se necessário presencial, mediante solicitação prévia da equipe do Órgão Contratante.

o) Apoio quanto a obstáculos operacionais e de planejamento, incluindo, sem limitação, a configuração dos componentes da solução, problemas de usabilidade, diagnósticos de problemas técnicos e análises de tendências associadas a solução e seus componentes.

p) Os serviços de operação assistida poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverão ser realizados nas dependências do Órgão Contratante, com profissional certificado e devidamente treinado na solução e poderá ser de segunda a sexta-feira, das 08h às 12h ou das 14h às 18h, à critério do Órgão Contratante, de modo que os trabalhos possam ser realizados com qualidade e eficácia, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe do Órgão Contratante, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

3.8. Será solicitado no mínimo, 1 (uma) sessão de operação assistida por trimestre, e no máximo 2 (duas) sessões por mês, devendo ocorrer a primeira logo após a implantação da solução e seus módulos de gerenciamento de acesso lógico privilegiado, para possibilitar a integração da solução com os dispositivos e credenciais privilegiadas existentes no ambiente do Órgão Contratante, que deverá ser realizada contemplando as categorias e passos listados abaixo:

a) Integração com ambiente de servidores Microsoft.

b) Integração com ambiente de estações de trabalho Microsoft.

c) Integração com ambiente de servidores Linux.

d) Integração com estações de trabalho Linux.

e) Integração com servidores de banco de dados

f) Integração com dispositivos de redes (firewalls, e outros).

3.9. O serviço deverá ocorrer durante toda a vigência contratual, e deverá ser disponibilizado pela CONTRATADA um sistema de acompanhamento e controle de chamados onde eles serão registrados com acesso liberado para cada integrante da

equipe técnica do Órgão Contratante que será informada a lista de integrantes no início da vigência contratual.

3.10. O sistema deverá permitir abertura de chamados via telefone, e-mail e/ou console de acesso web pela equipe do Órgão Contratante.

3.11. A Contratada deverá disponibilizar canal telefônico nacional, local, 0800 ou equivalente sem custo adicional para a Contratante, além de canais eletrônicos de abertura de chamados.

3.12. Os serviços serão prestados de forma remota observando as seguintes condições:

3.12.1. O suporte poderá ser prestado por telefone, e-mail, chat ou internet, prioritariamente serão abertos os chamados via e-mail.

3.12.2. Durante as sessões remotas a CONTRATADA deverá utilizar ferramenta própria para acesso remoto seguro ao ambiente do Órgão Contratante, possibilitando a gravação das sessões remotas e possibilitando o acesso simultâneo de todos os envolvidos na solução de cada chamado, seguindo todas as diretrizes de segurança pré-estabelecidas.

3.13. Para chamados de severidade Crítica, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

Severidade	Descrição	Prazo máximo de início de atendimento remoto	Solução de Contorno	Prazo máximo da solução
Urgente / Crítica Severidade (1)	Situação emergencial ou problema crítico que cause indisponibilidade do ambiente.	Até 1 (uma) hora após a abertura do chamado remoto.	Até 4 (quatro) horas	até 24h ou plano formal aprovado.
Alta Severidade (2)	Impacto de alta significância relacionado à utilização do ambiente: ocorrência de indisponibilidade de funcionalidade ou recurso importante onde as operações continuam de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Até 2 (duas) horas após a abertura do chamado remoto.	Até 8 (oito) horas	Até 3 (três) dias após abertura do chamado remoto.
Média Severidade (3)	Impacto de baixa significância relacionado à utilização do ambiente. Não há ocorrência de indisponibilidade de funcionalidade ou recurso, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 8 (oito) horas após a abertura do chamado remoto.	até 2 (dois) dias	Até 5 (cinco) dias após abertura do chamado remoto.
Baixa Severidade (4)	Consulta e/ou dúvida técnica e/ou transferência de conhecimento	Até 24 (vinte e quatro) horas após a abertura do chamado remoto.	não aplicável	Até 10 (dez) dias após a abertura do chamado remoto.

3.14. Não haverá limite para chamados relacionados ao escopo contratado.

3.15. O nível de severidade será atribuído pela equipe autorizada do Órgão Contratante no momento da abertura do chamado, podendo ser reavaliado mediante justificativa técnica da Contratada, desde que validado formalmente pela Contratante.

3.16. A suspensão da contagem de SLA somente poderá ocorrer mediante justificativa registrada no chamado, indicação objetiva da pendência impeditiva, comunicação à equipe técnica da Contratante e aceite formal da fiscalização técnica.

3.17. O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação de advertências formais e poderão ser aplicadas glosas, mediante apuração

administrativa, observados contraditório e ampla defesa, conforme tabela a seguir e serem descontadas da garantia financeira dos serviços prestados:

Resultado esperado e níveis de qualidade exigidos	Unidade de cálculo	Fórmula de cálculo da glosa	Limite da glosa
Crítica	1hora	$NHA * 0,7\% * VFM$	10% da VFM
Alta	1hora	$NHA * 0,5\% * VFM$	10% da VFM
Média	1hora	$NHA * 0,3\% * VFM$	10% da VFM
Onde: NHA = Número de horas de atraso após o término do prazo máximo esperado para solução. VFM = Valor da fatura no mês do suporte técnico mensal.			

3.18. Durante o período de vigência do contrato a CONTRATADA deverá apresentar mensalmente relatório em formato eletrônico, contendo todos os chamados ocorridos no mês e seus prazos de atendimento, contendo informações analíticas e sintéticas de cada chamado, contendo a lista e total de chamados concluídos dentro e fora do prazo de SLA estabelecido.

3.19. Deverá ser garantido ao Órgão Contratante pleno acesso às últimas atualizações e informações do FABRICANTE da solução, além de pleno acesso administrativo, observados os perfis autorizados e requisitos de segurança, sendo obrigação da CONTRATADA a abertura de qualquer chamado necessário junto a equipe de suporte do FABRICANTE, caso seja necessário, devendo possuir todos os acessos necessários para a execução dos serviços de suporte técnico com operação assistida e transferência de conhecimento.

3.20. A Contratada deverá apoiar o processo progressivo de integração dos ativos, contas privilegiadas, credenciais e dispositivos indicados pela Contratante, observando plano de Implantação aprovado pela fiscalização técnica.

Indicador	Fórmula de Apuração	Meta Referencial*	Periodicidade	Evidência
Cobertura de contas privilegiadas	Contas cadastradas no PAM / total de contas elegíveis	≥ 80% em 180 dias	Mensal	Relatório plataforma
Cobertura de ativos críticos	Ativos integrados / total ativos elegíveis	≥ 70% em 180 dias	Mensal	Inventário + PAM
Credenciais com rotação ativa	Credenciais rotacionadas / total credenciais elegíveis	≥ 75% em 180 dias	Mensal	Logs PAM
Sessões privilegiadas auditadas	Sessões gravadas / total sessões PAM	≥ 95%	Mensal	Trilhas auditoria
Uso efetivo da plataforma	Acessos via PAM / total acessos privilegiados mapeados	Evolução contínua	Mensal	Logs + SIEM
Contas órfãs identificadas	Quantidade detectada no mês	Informativo	Mensal	Relatório técnico
Contas órfãs tratadas	Contas saneadas / contas órfãs detectadas	≥ 80% em 90 dias	Mensal	Evidência tratamento
Tempo médio onboarding (**) conta crítica	Soma dias onboarding / nº contas críticas onboarded	≤ 15 dias	Mensal	Plano implantação
* Metas referenciais podem ser ajustadas pela Contratante conforme maturidade inicial do ambiente.				
** Onboarding é o processo de trazer um ativo, conta, sistema ou credencial para dentro da gestão da solução PAM, fazendo com que ele passe a ser controlado, monitorado e protegido pela plataforma.				

4. TREINAMENTO

4.1. A CONTRATADA deverá realizar treinamento à equipe técnica do Ministério que atuará com a solução, considerando 1 (uma) turma, para 10 (dez) servidores, além das transferências de conhecimentos que está prevista nos chamados de suporte técnico.

4.2. O treinamento poderá ocorrer de forma remota ou presencial, a critério do Órgão Contratante, devendo, nesse caso, ser realizado nas dependências do Órgão Contratante, com instrutor certificado na solução e deverá ter carga horária mínima de 8 (oito) horas, e poderá ser de segunda a sexta-feira, das 8h às 12h ou das 14h às 18h, de modo que os alunos possam absorver os conhecimentos oficiais do fabricante acerca da solução adquirida, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA.

4.3. Para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe do Órgão Contratante, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

4.4. O conteúdo do Treinamento e a carga horária, devem obedecer às condições abaixo descritas:

4.4.1. Treinamento para a solução de gerenciamento de acesso lógico privilegiado

4.4.2. Carga Horária mínima Total: 08 (oito) horas

4.4.3. Participantes: 10 pessoas.

4.5. A CONTRATADA deverá apresentar um Plano de Treinamento (ementa) para avaliação da CONTRATANTE, com vistas a capacitar a equipe que irá interagir com a solução de gerenciamento de acesso lógico privilegiado, sendo que o planejamento das datas e horários de execução do treinamento deverá ser acordado entre a CONTRATADA e a CONTRATANTE.

4.6. O treinamento deverá contemplar, no mínimo, administração da solução, configuração de políticas, gestão de credenciais, gravação e auditoria de sessões, geração de relatórios, integração com diretórios, boas práticas de segurança, operação assistida e tratamento de incidentes.

4.7. A CONTRATADA deverá disponibilizar treinamento com vistas à capacitação

técnica de carácter teórico-prático para a equipe técnica da CONTRATANTE, compreendendo as tecnologias envolvidas na solução contratada, assim como capacitação nos produtos utilizados para atender aos requisitos das especificações técnicas.

4.8. A CONTRATADA deverá disponibilizar os manuais, tutoriais e vídeos para consulta, que tratam dos principais tópicos da Solução.

4.9. Todos os materiais entregues, disponibilizados e utilizados para o Treinamento, bem como os disponibilizados para consulta, serão concedidos com direito de uso interno e reprodução para fins exclusivos de capacitação interna da Contratante, para sua aplicação e uso em treinamentos internos.

4.10. Deverão ser fornecidos certificados para os servidores da CONTRATANTE que frequentarem pelo menos 85% (oitenta e cinco por cento) do total de horas de treinamento, devendo ser emitidos no idioma português e conterem a descrição da ementa do curso, carga horária, período de realização e nome completo do participante.

4.11. A CONTRATADA, ao término do Treinamento, deverá realizar a avaliação do curso ministrado com os servidores participantes, por meio de Questionário Avaliativo, devendo conter, no mínimo, os seguintes itens de avaliação:

- a) Avaliação geral do treinamento;
- b) Conteúdo do curso;
- c) Apresentação do conteúdo;
- d) Aplicabilidade no ambiente de trabalho;
- e) Carga horária;
- f) Material didático;
- g) Recursos utilizados;
- h) Didática e conhecimento do profissional;
- i) Observações.

4.12. Para fins de avaliação do Treinamento, o questionário deverá conter, para cada item de avaliação (letras “a” a “h”), as seguintes alternativas: Ótimo; Bom; Razoável; Ruim e Péssimo; devendo conter espaço para que os servidores manifestem suas considerações em relação à alternativa escolhida.