Estudo Técnico Preliminar 39/2023

1. Informações Básicas

Número do processo: 53115.017854/2023-07

2. Descrição da necessidade

Solução de Gerenciamento de Acesso Lógico Privilegiado

2.1 Motivação/Justificativa

2.1.1 O Ministério das Comunicações é um órgão da administração federal direta que foi criado em junho de 2020, a partir do desmembramento do Ministério da Ciência, Tecnologia e Inovações. A pasta foi criada com o objetivo de fortalecer as áreas de política nacional de telecomunicações, política nacional de radiodifusão; e, serviços postais, telecomunicações e radiodifusão.

2.1.2 Além disso, é de competência do Ministério atuar na política de comunicação e divulgação do Governo Federal; no relacionamento do Governo Federal com a imprensa regional, nacional e internacional; convocação de redes obrigatórias de rádio e televisão; bem como na pesquisa de opinião pública; e no sistema brasileiro de televisão pública.

2.1.3 No que tange a adoção de uma tecnologia de gerenciamento de acesso lógico privilegiado, o MCOM deseja contratar uma solução que seja baseada em software e se adapte ao ambiente atual já em produção, aproveitando todo o investimento já realizado em hardware, racks, sala cofre, sistemas de virtualização, sistemas de banco de dados, políticas e softwares de backup e segurança, dentre outros, possibilitando sua expansão de capacidade por meio da infraestrutura já existente, não sendo necessário qualquer custo adicional com gerenciamento e manutenção de hardware ou novo custo com consumo de energia elétrica ou espaço físico. Dessa forma, com vistas a apoiar as atividades dos usuários de TIC, faz-se necessária a contratação dos serviços que cooperam para a operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação do MCOM.

2.1.4 O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da necessidade que consta no Documento de Formalização da Demanda n° 95/2023 (11067235), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o processo de contratação.

2.1.5 O mapa estratégico do MCOM 2021-2023, tem como missão “Ampliar a conectividade, aprimorar a qualidade dos serviços de comunicação e assegurar a prestação de informações governamentais essenciais à proteção da soberania nacional e ao exercício da cidadania”, de modo que permita à área de tecnologia da informação e comunicação do MCOM atender às demandas resultantes da necessidade de alinhamento das ações de tecnologia com o planejamento estratégico institucional.

2.1.6 A continuidade dos negócios e da prestação de serviços à sociedade pelo MCOM depende diretamente da garantia de atualização de versões e serviços correlatos, garantindo o aumento da segurança em acessos remotos e no ambiente computacional, de forma a contribuir para a proteção dos dados e a agilidade dos serviços prestados no ambiente tecnológico do Ministério. Nesse sentido, faz-se necessário uma nova solução de gerenciamento de acesso lógico privilegiado com vistas ao atendimento das demandas de infraestrutura dos usuários dos serviços oferecidos pelo Ministério.

2.1.7 A contratação pretendida encontra-se prevista no Plano Diretor de Tecnologia da Informação e Comunicação do MCOM, PDTIC 2023-2024 e encontra-se alinhada aos objetivos estratégicos definidos pelo Mapa Estratégico do MCOM 2021 – 2023 e no Plano Anual de Contratação – PAC, conforme tabela abaixo:

Caderno do Planejamento Estratégico Institucional 2021 -2023
Objetivo

Garantir recursos materiais e infraestrutura de TIC necessários ao desempenho das atribuições institucionais.			
Aprimorar a governança, a integridade, a gestão estratégica e a gestão da informação			
Alinhamento ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC			
Plano Diretor de Tecnologia da Informação e Comunicação – PDTCI 2023 - 2024			
ID	**NECESSIDADE**		
N2	Provimento e manutenção de soluções de TI		
N5	Aprimoramento dos processos de Segurança da Informação		
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
*	Prospectar solução para monitoramento das ações de governança e implantação da LGPD	M4	Prover soluções de TI
*	Prover soluções de segurança da informação e comunicações	M7	Prover e prospectar soluções e conscientização para segurança da informação
Alinhamento ao Plano de Contratação Anual - PCA			
Item no PAC	**Descrição**		
95/2023	Gerenciamento de Acesso Lógico Privilegiado		

2.1.8 Cabe registrar nesse Estudo Técnico algumas premissas necessárias e específicas do objeto que devem ser observadas dentro dos objetivos da contratação:

2.1.9 Norma Complementar n. 14/IN01/DSIC/GSIPR, que estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3. Área requisitante

Área Requisitante	Responsável
Coordenação Geral de Tecnologia da Informação e Comunicação	Helder Mota Gomes

4. Necessidades de Negócio

4.1 Identificação das necessidades de negócio

4.1.1 Seguindo as premissas acima, alinhadas com as necessidades do Ministério, essa contratação tem como objetivo atender as seguintes necessidades de negócio:

- Manter os Serviços de TI sempre disponíveis para seus usuários;
- Prestar atendimento adequado e satisfatório aos usuários do MCOM, possibilitando o pleno desenvolvimento de suas atividades;
- Adequado monitoramento e suporte destinados ao ambiente tecnológico do MCOM, buscando prevenir e corrigir falhas para garantir a integridade das informações e a estrutura desse ambiente de proteção.

4.1.2 Os impactos negativos decorrentes da não efetivação da presente contratação são:

a. 1. Interrupção na prestação dos serviços, acarretando perdas irreparáveis à administração e a própria população envolvida com a missão do MCOM.
b. 2. Indisponibilidade no atendimento ao usuário, sistemas, aplicações, serviços, integrações e portais do MCOM.
c. 3. Interrupção da sustentação, construção, implantação ou uso da solução de TI.
d. 4. Impossibilidade de execução dos serviços essenciais do Ministério.

5. Necessidades Tecnológicas

5.1 Identificação das necessidades tecnológicas

5.1.1 Atualmente, o MCOM não possui, uma solução de Gerenciamento de Acesso Lógico Privilegiado, disso advém a necessidade de contratação dessa solução objeto desse Estudo Técnico Preliminar - ETP, de forma a contemplar garantia de atualização de versões e serviços correlatos, conferindo ao MCOM uma melhoria significativa da segurança e do controle de acesso à informação sob responsabilidade, conforme condições, quantidades e exigências estabelecidas neste instrumento.

5.1.2 O gerenciamento de acesso lógico privilegiado é uma necessidade urgente do MCOM e essa necessidade se justifica também com base no fato de que essa adoção elevará a disponibilidade dos serviços técnicos promovendo um melhor atendimento a todos os usuários, independente dos locais físicos no qual se encontrem. Ademais, todos os acessos remotos passarão a ser auditados, possibilitando que todas as ações realizadas possam ser consultadas até mesmo pelo usuário final que poderá receber o atendimento em qualquer localização nacional, incluindo a possibilidade de acesso para atendimento a dispositivos móveis como smartphones.

5.1.3 De acordo com o último levantamento realizado, atualmente, o MCOM possui um total de 1.640 (três mil quinhentos e quarenta) dispositivos, sendo aproximadamente 1.290 estações de trabalho, 300 servidores físicos e virtuais e 50 aplicações web. O atendimento a toda essa estrutura é realizada de três maneiras: por telefone, presencialmente ou virtualmente. Quando realizado de maneira remota, esse atendimento ocorre sem uma conexão segura ou criptografada e sem a geração de uma trilha de auditoria para averiguação futura das ações dos técnicos internos e/ou terceirizados externos, dentro do ambiente computacional do Ministério, porque não há um mecanismo lógico que gerencie de forma efetiva e segura todos os acessos remotos. Por meio da aquisição pretendida, visa-se otimizar a utilização dos recursos humanos disponíveis, pois não haverá a necessidade de locomoção até o espaço físico destino e cada atendente poderá atender vários chamados ao mesmo tempo utilizando a nova opção tecnológica.

5.1.4 Além disso, será possível implementar uma comunicação mais eficiente e segura entre os técnicos e os usuários finais, elevando o nível de disponibilidade, integridade e confiabilidade das informações custodiadas pelo MCOM, criando regras de segurança e rastreabilidade das conexões de acesso remoto. A solução descrita constitui tecnologia de gerenciamento de acesso lógico privilegiado amplamente necessária para o MCOM. A não adoção, impactará fortemente no controle e auditoria do uso de credenciais privilegiadas por meio dos acessos remotos realizados e na proteção das informações e no aumento da segurança e agilidade nos serviços prestados ao cidadão por meio de suas políticas públicas. Por outro lado, uma vez adotada essa tecnologia haverá significativa elevação da disponibilidade dos técnicos promovendo um melhor atendimento a todos os usuários, independente dos locais físicos no qual se encontrem. Ademais, todos os acessos lógicos remotos passarão a ser auditados.

5.1.5 No que tange à adoção de uma tecnologia de gerenciamento de acesso lógico privilegiado, o MCOM objetiva contratar uma solução que seja baseada em software e se adapte ao ambiente atual já em produção, aproveitando todo o investimento já realizado em hardware, racks, sala cofre, sistemas de virtualização, cofre de senhas, políticas e softwares de backup e segurança,

dentre outros, possibilitando a expansão de capacidade por meio da infraestrutura já existe, não sendo necessário qualquer custo adicional com gerenciamento e manutenção de hardware.

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

6.1 Requisitos Legais

6.1.1 O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis.

6.1.2 A contratada deverá se submeter à Política de Segurança da Informação (POSIC) do Ministério das Comunicações, nos termos da Portaria MCOM nº 2.454 de 22 de abril de 2021.

6.2 Requisitos Temporais

6.2.1 Início da cobertura da prestação de serviço anual de subscrição da solução de gerenciamento de acesso lógico privilegiado com garantia de atualização de versões, iniciando no 1º dia útil após a assinatura do contrato e finalizado no último dia da primeira vigência do contrato, podendo se repetir até o final de cada período de 12 (doze) meses, até o limite de 60 (sessenta) meses.

6.2.2 Instalação e configuração inicial a solução para deixá-la funcional e com a cobertura do serviço de subscrição das licenças devidamente aplicadas, funcionais e vigentes, iniciando no 1º dia útil após a assinatura do contrato e finalizado em até 10 (dez) dias úteis contados da data de assinatura do contrato.

6.2.3 Configuração e integração da solução com os dispositivos e credenciais do ambiente do MCOM por meio da criação e testes das políticas necessárias para a integração, iniciando no 1º dia útil após o término da instalação e configuração inicial da solução e finalizando 30 (trinta) dias úteis contados da data de assinatura do contrato.

6.2.4 O serviço de suporte técnico com operação assistida para solução iniciará em até no 1º dia útil após a finalização da instalação e configuração da expansão do licenciamento da solução e finalizando até o último dia da primeira vigência anual do contrato, se repetindo anualmente a cada avaliação do fornecedor ao final de cada período de 12 (doze) meses, até o limite de 60 (sessenta) meses.

6.3 Requisitos Tecnológicos

6.3.1 Preservação do investimento já realizado - No que tange a adoção de uma tecnologia de gerenciamento de acesso lógico privilegiado, o MCOM deseja contratar uma solução que seja baseada em software e se adapte ao ambiente atual já em produção, aproveitando todo o investimento já realizado em hardware, racks, sala cofre, sistemas de virtualização, sistemas de banco de dados, políticas e softwares de backup e segurança, dentre outros, possibilitando sua expansão de capacidade por meio da infraestrutura já existente, não sendo necessário qualquer custo adicional com gerenciamento e manutenção de hardware ou novo custo com consumo de energia elétrica ou espaço físico.

6.3.2 Continuidade de Negócio – Aquisição de solução, contemplando solução de gerenciamento de acesso lógico privilegiado, contemplando garantia de atualização de versões e serviços correlatos de suporte técnico e apoio técnico com transferência de conhecimento.

6.3.3 A solução promoverá uma melhor integração entre as áreas e espaços físicos que compõem o MCOM, elevando a disponibilidade dos técnicos para melhor atendimento a todas as demandas, auditando todos os acessos remotos e todas as ações realizadas, onde poderão ser consultadas até mesmo pelo usuário final que poderá receber o atendimento em qualquer localização física que esteja, incluindo a possibilidade de acesso para atendimento a dispositivos móveis como smartphones.

6.3.4 A solução deve possibilitar realizar login usando duplo fator de autenticação possibilitando usar software não pago como o Google Authenticator.

6.3.5 A solução deve possibilitar habilitar a gravação de sessões de compartilhamento de tela e linha de comando, no mínimo.

6.3.6 A solução de ser capaz de se comunicar de forma "peer-to-peer" para sessões de compartilhamento de tela, transferência de arquivos ou shell remoto. Caso naquele momento a solução não consiga conectar de forma "peer-to-peer", a solução deve criar uma conexão se utilizando da console de origem como intermediária.

6.3.7 A solução deve possibilitar quando necessário nos atendimentos remotos, gerenciar senhas com altos poderes de acesso do MS Active Directory e em ambientes Linux e Unix, Bancos de Dados.

6.3.8 A solução deve ser capaz de direcionar as sessões de acesso remoto de suporte em uma fila de atendentes disponíveis quando necessário e transferir uma sessão de suporte para outro representante técnico se necessário.

6.3.9 A solução deve suportar a definição de políticas de composição de senhas, quando necessário para os acessos remotos e suas necessidades de acesso.

6.3.10 A solução deve permitir iniciar sessões remotas a dispositivos não assistidos, ou seja, dispositivos do ambiente de produção do MCOM, onde não existam usuários solicitando suporte.

6.3.11 A solução deve permitir visualizar todas as telas de um cliente com mais de um monitor habilitado em caso de múltiplos monitores.

6.3.12 A solução deve possibilitar a apresentação de pesquisa de satisfação com ao cliente após a finalização de cada sessão de suporte.

6.4 Requisitos de Segurança

6.4.1 A solução deve possibilitar configurar scripts para serem executados em qualquer sessão de compartilhamento de tela ou compartilhamento de shell.

6.4.2 A solução deve possibilitar configurar, que, ao iniciar a sessão, o mouse e o teclado iniciem de forma restrita ao representante de suporte.

6.4.3 A solução deve permitir chat entre o atendente e o usuário final quando necessário, atendente e outros atendentes, além de possibilitar a criação e utilização de mensagens pré-cadastradas.

6.4.4 A solução deve permitir configurar quanto tempo um representante de suporte pode permanecer inativo até que seja desconectado de forma automática da console.

6.4.5 A solução deve permitir que os representantes de suporte possam se autenticar em no mínimo os seguintes serviços: LDAP, Active Directory, RADIUS, SAML e Kerberos.

6.5 Requisitos de Instalação

6.5.1 Compreende-se nesta etapa a instalação e configuração inicial da solução para deixá-la funcional e com a cobertura do serviço de subscrição das licenças devidamente aplicadas, funcionais e vigentes, que deverá ser realizada em no máximo 10 (dez) dias úteis contados da data de assinatura do Contrato.

6.5.2 Durante esta etapa, a equipe da Contratada deverá estar presente, nos horários de instalação definidos pelo MCOM e nos casos de atuações remotas, deverá pré-agendar com a equipe do MCOM os horários e acessos necessários de acordo com as políticas e diretrizes de segurança do MCOM.

6.5.3 As atividades de instalação e configuração inicial da solução, poderão ser executadas em horário comercial, período noturno ou finais de semana, de acordo com a definição do MCOM.

6.5.4 Para esta etapa o MCOM disponibilizará a infraestrutura de hardware e software necessários e já existente em seu ambiente, incluindo o ambiente virtualizado e banco de dados.

6.5.5 Não será fornecido e/ou disponibilizado qualquer sistema operacional para compor o funcionamento da solução, isso deverá ser por conta da licitante.

6.6 Suporte Técnico com operação assistida

6.6.1 O atendimento de suporte para a solução será do tipo telefônico e/ou internet 24 (vinte e quatro) horas por dia e sete dias por semana, e deverá ser realizado por profissionais especializados e cobrir todo e qualquer defeito e/ou dúvida apresentada e não estará contemplado problemas relacionados a hardware, uma vez que os recursos físicos serão de responsabilidade do MCOM.

6.6.2 O 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.

6.6.3 As atividades de suporte técnico serão realizadas, a critério do MCOM, em suas dependências em Brasília-DF, a partir da assinatura do Contrato e durante toda sua vigência contratual.

6.6.4 Não estão contemplados problemas relacionados a hardware, uma vez que os recursos físicos serão de responsabilidade do MCOM.

6.6.5 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 MCOM, além do desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:

- Orientação sobre acesso, o uso, a configuração, a instalação da solução e a integração com os dispositivos do MCOM, contando com acesso ao conhecimento privilegiado de recursos da Contratada e quando necessário do fabricante da solução.
- Orientação quanto às melhores práticas para implementação e integração da solução no ambiente do MCOM.
- Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões da solução e seu impacto no gerenciamento dos acessos lógicos remotos e privilegiados no ambiente do MCOM.
- Análise técnica qualificada nas análises e prevenções de vulnerabilidades encontradas e passíveis de serem exploradas na solução de gerenciamento de acesso lógico.
- Aplicação de melhores práticas para implementação do gerenciamento de acesso lógico remoto e privilegiado.
- Realização de estudos e configuração do ambiente e implementação das integrações necessárias, instáveis ou com comportamento errático caso aconteçam
- Realização de estudos para melhoria dos acessos lógicos do ambiente atual do MCOM.
- Implementação de novas integrações que não tenham ainda sido efetivadas ou sejam necessárias.
- Identificação de melhorias e respectivo tratamento (melhoria de parametrização).
- Parametrização da solução, de acordo com as regras e políticas de acessos lógicos remotos e privilegiados definidos pelo MCOM
- Apoio na elaboração e adequação de relatórios executivos, gerenciais, de auditoria e operacionais quando necessário.
- Suporte avançado para estratégia e planejamento no gerenciamento de acessos lógicos remotos e privilegiados por meio da solução ao ambiente do MCOM.
- Avaliação e comparação de novas funcionalidades de forma remota e se necessário presencial, mediante solicitação prévia da equipe do MCOM.
- 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.

6.6.6 O MCOM poderá solicitar durante toda a vigência contratual do serviço, transferência de conhecimento e/ou operação assistida de segunda a sexta-feira em horário comercial como parte integrante do serviço prestado, para isso poderá ser solicitado sessões remotas e/ou presenciais, bem como workshops de transferência de conhecimento para a equipe, para isso serão abertos chamados com severidade “4” classificado como “baixa”.

6.6.7 As transferências de conhecimento poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverá ser realizado nas dependências do MCOM, com instrutor certificado na solução e deverá ter carga horária mínima de 04 (quatro) horas, e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério do MCOM, 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, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe do MCOM, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a Contratada.

6.6.8 Serão solicitados workshops de transferência de conhecimento, sendo uma ao final da implantação da solução com os módulos de gerenciamento de acesso lógico privilegiado, para possibilitar a transferência dos conhecimentos para toda a equipe em tempo de execução com a solução funcionando, em produção e devidamente integrada ao ambiente do MCOM e no máximo 1 (uma) workshop de transferência de conhecimento por mês caso a equipe do MCOM entenda que seja necessário.

6.6.9 Para os casos em que houver alguma mudança significativa de atualização de versão, que reflita na operação da solução, a Contratada deverá transferir este conhecimento para equipe interna do MCOM sempre que ocorrer, para estes casos serão também abertos chamados de severidade “4”.

6.6.10 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 MCOM, com profissional certificado e devidamente treinado na solução e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério do MCOM, 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 MCOM, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a Contratada.

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

- Integração com ambiente de servidores Microsoft.
- Integração com ambiente de estações de trabalho Microsoft.
- Integração com ambiente de servidores Linux.
- Integração com estações de trabalho Linux.
- Integração com servidores de banco de dados
- Integração com dispositivos de redes (firewalls, switches e outros).

6.6.12 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 MCOM que será informada a lista de integrantes no início da vigência contratual.

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

6.6.14 Em casos de chamados abertos via telefone, o sistema deverá disponibilizar um número local onde o MCOM possui sua sede (Brasília-DF), evitando custos desnecessários, onde o número deverá ser disponibilizado pela Contratada no formato 0800 ou (061)+(número local) e deverá possibilitar a abertura de chamados por meio de gravação de áudio, caso os atendentes estejam ocupados no momento da ligação, devendo o sistema identificar o número utilizado pré-cadastrado e liberado para abertura de chamados que serão automaticamente abertos e enviados para uma fila de atendimentos apropriada, devendo registrar o horário do momento da ligação como horário de abertura do chamado em questão.

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

- O suporte poderá ser prestado por telefone, e-mail, chat ou internet, prioritariamente serão abertos os chamados via e-mail.
- Durante as sessões remotas a Contratada deverá utilizar ferramenta própria para acesso remoto seguro ao ambiente do MCOM, 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.
- 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	Prazo máximo da solução
Urgente / Crítica **Severidade 1**	Situação emergencial ou problema crítico que cause indisponibilidade do ambiente.	Até 2 (duas) horas após a abertura do chamado remoto.	Até 72 (setenta e duas) horas após abertura do chamado remoto.
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 4 (quatro) horas após a abertura do chamado remoto.	Até 5 (cinco) dias após abertura do chamado remoto.
Normal **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 8 (oito) 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.	Até 10 (dez) dias após a abertura do chamado remoto.

6.6.16 Não haverá limite para o número de chamados de suporte técnico.

6.6.17 O nível de severidade será atribuído pela equipe autorizada do MCOM no momento da abertura do chamado e poderá ser reclassificado pela equipe da contratada caso seja necessário.

6.6.18 Durante os atendimentos dos chamados, para efeitos de apuração do tempo despendido para solução, serão desconsiderados os períodos em que o MCOM estiver responsável por executar alguma ação necessária para a análise e solução da ocorrência ou quando for necessário aguardar alguma correção por parte do fabricante que não impacte no funcionamento e utilização do ambiente, sendo permitido nestes casos pausar ou interromper o chamado, mas sem alterar o número inicial de protocolo/número de abertura do mesmo.

6.6.19 O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação de advertências formais e caso seja definido pelo MCOM poderão ser aplicadas glosas 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

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.

6.6.20 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.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 Relação entre a demanda e a quantidade de bens/serviços a serem contratados:

7.1.1 Para o correto dimensionamento da quantidade de bens e serviços a serem contratados, a equipe de planejamento da contratação levantou o volume de dispositivos do Ministério.

7.1.2 Os acessos remotos para suporte aos usuários do ambiente do MCOM requerem hoje no máximo 10 (dez) conexões simultâneas dos usuários atendentes terceirizados e internos, a demanda para acesso ao ambiente de produção do MCOM, será de no máximo 1.640 (Mil seiscentos e quarenta) dispositivos conectados de forma remota simultaneamente ao ambiente do MCOM. Face ao exposto a estimativa da demanda, deverá observar os itens e quantitativos da tabela abaixo:

Item	Descrição	Unidade de Medida	Quantidade
1	Subscrição anual da solução para atendente, com garantia de atualização de versões – para suporte remoto de até 10 usuários simultâneos para até 1.290 dispositivos (estações de trabalho).	Usuários	1
2	Subscrição anual da solução para dispositivo, com garantia de atualização de versões – para acesso ao ambiente de produção para até 400 dispositivos independente da quantidade de usuários simultâneos.	Dispositivos	1
3	Serviço de suporte técnico com operação assistida.	Serviço Mensal	12
4	Treinamento (Turma de 5 alunos)	Turma	1

8. Levantamento de soluções

A análise comparativa de soluções, nos termos do inc. II do art. 11º da IN SGD/ME nº 94/2022, visa a elencar as alternativas de atendimento à demanda, considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

8.1 Identificação das Soluções

8.1.1 O Trabalho híbrido e os processos de negócios digitais na nuvem introduziram novos riscos. Atualmente, 60% dos trabalhadores do conhecimento são remotos e pelo menos 18% não retornarão ao escritório. Essas mudanças na maneira como trabalhamos, juntamente com o maior uso da nuvem pública, cadeias de suprimentos altamente conectadas e uso de sistemas ciberfísicos expuseram novas e desafiadoras “superfícies” de ataque. Isso deixa as organizações mais vulneráveis a ataques. Os sistemas de identidade estão sob ataque sustentado, o uso indevido de credenciais agora é o principal método que os invasores usam para acessar sistemas e atingir seus objetivos. Por exemplo, na violação da SolarWinds , os invasores usaram o acesso privilegiado de um fornecedor para se infiltrar na rede de destino.

8.1.2 O Gartner recomenda que os líderes de segurança olhem além das abordagens tradicionais de monitoramento, detecção e resposta de segurança para gerenciar um conjunto mais amplo de riscos. Além disso, usa o termo detecção e resposta a ameaças

de identidade (ITDR) para descrever uma coleção de ferramentas e processos para defender sistemas de identidade. A longo prazo, surgirão soluções mais consolidadas.

8.1.3 Ainda seguindo orientações do Gartner, alertou, por meio de um novo estudo global, que os líderes de segurança cibernética precisam adotar novas práticas, já que a responsabilidade sobre os riscos cibernéticos estão avançando para além das áreas de TI. “Os líderes de segurança cibernética estão esgotados, sobrecarregados e no modo ‘sempre ativo’”, alerta Sam Olyaei, diretor de pesquisa do Gartner. “Este é um reflexo direto de quão elástico o papel desse especialista se tornou na última década, devido ao crescente das expectativas entre as partes interessadas dentro de suas organizações.”, finaliza.

8.1.4 Em outra pesquisa realizada pelo Gartner, cerca de 88% dos conselhos consideram a segurança cibernética como um risco comercial e não apenas um problema técnico de TI. 13% dos entrevistados responderam que as empresas deveriam criar comitês específicos de segurança cibernética supervisionados por um diretor. O Gartner prevê que pelo menos 50% dos C-Levels terão requisitos de desempenho relacionados ao risco e gestão de segurança cibernética incorporados em seus contratos de trabalho até 2026. Isso afeta a pontualidade e a qualidade das decisões de risco das informações, que estão sendo cada vez mais tomadas por partes interessadas e fora da linha de visão da TI ou da segurança.

8.1.5 Para que as empresas tenham sucesso, o Gartner almeja uma mudança nas estratégias de negócios devido aos riscos na internet, destacando que o trabalho do líder de segurança cibernética é fundamental. “O papel desse profissional deve evoluir de ser a pessoa responsável pelo tratamento de riscos cibernéticos, para ser responsável por garantir que os líderes empresariais tenham as capacidades e o conhecimento necessários para tomar decisões informadas e de alta qualidade sobre riscos de informações”, afirma Olyaei. Outra constatação da pesquisa é de que investidores e regulamentação governamental incentivam organizações a adotarem o ESG também na segurança cibernética, relatando metas e métricas de segurança dentro de seus esforços ambientais, sociais e de governança como um requisito de negócios.

8.1.6 Como resultado, o Gartner prevê que 30% das grandes organizações terão metas ESG compartilhadas publicamente com foco em segurança cibernética até 2026. Segundo observações do diretor de pesquisa do Gartner, Claude Mandy, “as expectativas de que as organizações deveriam ser mais transparentes sobre seus riscos de segurança que aumentaram, resultando na demanda pública por maior transparência em seus relatórios ESG.

8.1.7 A cibersegurança não é mais apenas um risco para a organização, mas um risco social.” Afim de materializar e tornar mais fácil o entendimento, o Gartner listou 7 tendências para a cibersegurança, que devem se tornar grandes diferenciais para o sucesso e bom desempenho das empresas:

- Ampliação das áreas que precisam ser controlada: As organizações devem olhar para além das abordagens tradicionais de monitoramento, detecção e resposta de segurança, de forma a garantir a proteção de suas operações. Isso porque inovações como aplicativos em nuvem, cadeias de suprimentos digitais complexas, aplicativos de código aberto, entre outras, podem aumentar a vulnerabilidade.
- Atenção à cadeia digital de suprimentos: O Gartner prevê que até 2025, 45% das organizações em todo o mundo terão sofrido ataques em suas cadeias de suprimentos de software, um aumento de três vezes em relação a 2021. Por isso, é fundamental desde já ampliar os sistemas de proteção e também promover mudanças na cultura organizacional, conscientizando os colaboradores sobre os riscos digitais.
- Cuidado com identidade digital: Com dados armazenados em nuvem, é preciso ter, cada vez mais, sistemas sofisticados de controle de acesso, de forma que somente pessoas autorizadas consigam entrar na rede e comportamentos considerados suspeitos sejam analisados.
- Controle de riscos descentralizado: Segundo o Gartner, até 2025, uma função de segurança cibernética única e centralizada não será ágil o suficiente para atender às necessidades das organizações digitais. “Os gestores devem reconceituar sua responsabilidade para capacitar os Conselhos de Administração, CEOs e outros líderes de negócios a tomar suas próprias decisões de risco”, apontou o estudo. A consultoria aponta que 70% dos CEOs exigirão uma cultura de resiliência organizacional para sobreviver a ameaças decorrentes de crimes cibernéticos, eventos climáticos severos, distúrbios civis e instabilidades políticas, até 2025.
- Informação compartilhada: A mudança de cultura corporativa, aliada à melhor conscientização sobre os riscos e conhecimento de medidas de proteção será o grande diferencial das empresas para evitarem ataques. É preciso promover novas formas de pensar e incorporar novos comportamentos para garantir estratégias mais seguras de trabalho.
- Fornecedores precisam estar alinhados às estratégias de segurança: De nada adianta uma organização investir na mudança de cultura interna e em meios adequados de proteção às novas ameaças se os fornecedores não estão alinhados a este propósito. A preocupação deve fazer parte de toda a cadeia de valor da empresa.
- Proteção integrada é essencial para a cibersegurança: O Gartner aponta que as empresas precisam investir em uma arquitetura de malha de segurança cibernética (CSMA) para proteger todos os ativos, sejam eles locais, em data centers ou na nuvem.

8.1.8 A seguir apresentamos algumas soluções identificadas através de buscas na Internet ou pela leitura de estudos de mercado utilizados pelo Gartner.

- LogMein – www.logmain.com
- Zoom Meetings – www.zoom.us
- TeamViewer – www.teamviewer.com
- BeyondTrust – www.beyondtrust.com/remote-support

8.1.9 A tabela a seguir apresenta o levantamento de possíveis soluções:

Solução	Descrição
Solução A - Desenvolvimento próprio da solução	Desenvolvimento próprio, no Ministério, através de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais, para o atendimento das necessidades
Solução B - Solução de Software Livre	Utilização de solução de Software Livre que atenda a todos os requisitos da solução
Solução C - Contratação de nova solução	Contratação de solução (software proprietário) com licenciamento pago por subscrição/aluguel.

9. Análise comparativa de soluções

9.1 Solução A - Desenvolvimento próprio da solução

9.1.1 Esta alternativa é caracterizada pelo desenvolvimento próprio dessa solução no Ministéro, por meio de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais, para o atendimento das necessidades. No entanto, analisando-se a relação custo-benefício, percebe-se que uma solução com essas características seria altamente custosa /onerosa para ser desenvolvida internamente por meio do contrato de Fábrica de Software vigente.

9.2 Solução B - Solução de Software Livre

9.2.1 Software livre é um tipo de software que vem com permissão para cópia, uso e distribuição, com ou sem modificações, de forma gratuita ou por um preço. De forma geral, isso significa que o código-fonte deve estar disponível. A maioria dos softwares livres é licenciada por meio de uma licença livre, sendo o tipo GNU GPL a mais conhecida. As licenças de software livre permitem que eles sejam vendidos, mas estes em sua grande maioria estão disponíveis gratuitamente.

9.2.2 Software gratuito ou freeware é qualquer programa de computador cuja utilização não implica o pagamento de licenças de uso ou royalties. É importante não confundir o free de freeware com o free de free software, pois no primeiro uso o significado é de gratuito, e no segundo de livre. Um programa licenciado como freeware não é necessariamente um software livre, pode não ter código aberto e pode acompanhar licenças restritivas, limitando o uso comercial, a redistribuição não autorizada, a modificação não autorizada ou outros tipos de restrições. O freeware diferencia-se do shareware, no qual o usuário deve pagar para acessar a funcionalidade completa ou tem um tempo limitado de uso gratuito.

9.2.3 Foram encontradas algumas soluções de software livre ou gratuitos, porém todas pouco aderentes ao que se deseja dessa contratação:

a) O AnyDesk é um programa alemão da GmbH gratuito e fácil de usar. Para espelhar a tela de um computador em outra máquina, não há a necessidade de nenhuma configuração. Apenas informar o endereço do dispositivo que deseja acessar para liberar o acesso remoto. Ele tem uma interface simples e fácil de usar, porém, a desvantagem é que ele não possui chat, um diferencial dos concorrentes, que serve para os dois computadores se comunicarem enquanto o acesso ocorre.

- Pode ser usado gratuitamente, apenas para uso individual e avaliação.
- Não possui chat
- Não permite injeção de senhas de forma automática.
- Atende parte dos requisitos desejados, porém, encontramos apenas suporte na Alemanha.

b) TeamViewer (www.teamviewer.com) - é um dos programas de maior sucesso entre os usuários que precisam de acesso remoto para computador. Sua versão gratuita é básica e tem várias limitações.

- Limitado gratuitamente a 1 dispositivo.
- Não permite a injeção de senhas de forma automática
- Não atende a grande maioria das necessidades, em especial em função de sua limitação a conexões simultâneas e quantidade máxima de dispositivos.

c) Podem existir outros softwares livres que poderiam atender parte dos requisitos levantados pelo requisitante da solução, mas não há uma ferramenta que atenda toda a necessidade ou grande parte dos requisitos, bem como é necessário a compor várias Soluções para atendimento ao pleito, tais como:

- - LogMein – www.logmain.com
- - Zoom Meetings – www.zoom.us

9.3 Solução C - Contratação de solução de mercado (software proprietário):

9.3.1 De acordo com as necessidades levantadas e após realização de estudos, somente soluções de software proprietário poderiam atender as necessidade do MCOM.

9.3.2 O objeto proposto para a contratação pretensa constitui o fornecimento de solução de gerenciamento de acesso lógico privilegiado, contemplando garantia de atualização de versões e serviços correlatos, provendo ao MCOM uma melhoria significativa da segurança e controle de acesso à informação sob sua responsabilidade, conforme condições, quantidades e exigências estabelecidas neste instrumento.

9.3.3 É importante prever uma ferramenta que possa criar trilhas de auditoria por meio de logs e gravação das ações realizadas durante um atendimento por meio de um acesso remoto, possibilitando auditar as atividades dos acessos remotos ao ambiente de rede do MCOM, além de possibilitar atendimentos remotos para dispositivos móveis smartphones de forma segura e criptografada.

9.3.4 Uma das necessidades também da equipe de TI do Ministério é possibilitar a injeção automática de senhas, permitindo que os usuários autentiquem 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, e ao acessar um ativo baseado em Windows ou Linux, a injeção de credenciais deve ser suportada na tela de login de forma integrada, garantido assim a proteção das senhas e impedindo ataques do tipo ransomware que necessitam de credenciais privilegiadas para executar o ataques deste tipo.

Requisito	Solução	SIM	NÃO	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução A			X
	Solução B	X		
	Solução C	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução A			X
	Solução B			X

	Solução C			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução A			X
	Solução B	X		
	Solução C			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução A			X
	Solução B			X
	Solução C			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução A			X
	Solução B			X
	Solução C			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução A	X		
	Solução B	X		
	Solução C	X		

10. Registro de soluções consideradas inviáveis

10.1 Em conformidade com § 1º do art. 11 da IN SGD 94/2022, as soluções identificadas e consideradas inviáveis estão registradas nesse Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade (Total Cost Ownership – TCO). Seguem abaixo as soluções consideradas inviáveis com as devidas justificativas que concluíram pela inviabilidade.

10.2 Após o levantamento das possíveis soluções, a equipe de planejamento da contratação conclui que as soluções inviáveis correspondem a:

Solução	Justificativa
	Relacionado à possibilidade de desenvolvimento da solução com a utilização da fábrica de software contratada pelo Ministério, a não utilização dessa solução é justificada ainda pelo fato de que o Ministério da Economia, traz orientações pela publicação do manual *"Boas práticas, vedações e orientações para contratação de serviços de desenvolvimento e manutenção*

Solução A - Desenvolvimento próprio da solução	*de software (Fábrica de Software)"*, disponível em desenvolvimento e manutenção de software, o seguinte: 1. Antes de decidir pela contratação de serviço de desenvolvimento de software ou pela abertura de projetos de desenvolvimento de software, a Equipe de Planejamento da Contratação ou a Equipe de Gestão de Projetos do órgão deve realizar Estudo Técnico Preliminar, nos termos do disposto no art. 12 da Instrução Normativa SLTI/MP nº 4, de 11 de setembro de 2014, e executar as seguintes atividades: 1.5. Analisar a viabilidade de contratação de software proprietário. 1. 5. É vedada a utilização dos serviços contratados para o desenvolvimento de softwares de atividades-meio. 2. 2.1. 1. São considerados softwares de atividades-meio os que são utilizados para apoio de atividades de gestão ou administração operacional, como, por exemplo, softwares de recursos humanos, ponto eletrônico, portaria, biblioteca, gestão de patrimônio, controle de frotas, gestão eletrônica de documentos, e que não têm por objetivo o atendimento às áreas finalísticas para a consecução de políticas públicas ou programas temáticos. 3. 2. Os softwares de atividades-meio devem ser adquiridos no mercado por meio de adoção de software público ou livre, contratação de software como serviço, ou software licenciado. O desenvolvimento de uma solução para atender ao objetivo deste estudo está alinhada à vedação exposta no item 3.5 do manual. Diante do exposto, não é recomendado o desenvolvimento interno da solução. Além disso, importante destacar que o custo- benefício para desenvolvimento interno de uma solução deste tipo com todas as funcionalidades necessárias não seria viável técnica e economicamente. Pelos motivos apresentados, este cenário não é recomendado para atender as necessidades do MCOM.
Solução B - Solução de Software Livre	As ferramentas de sosftware livre não se demonstraram viáveis, visto que seu uso não é corporativo (possui limitação de acesso, que é apenas individual) e suas funcionalidades não atendem à completude do que se necessita para o Ministério, visto que nãotratam da proteção dos acessos privilegiados. Ainda, nenhuma delas permite a injeção de senhas de forma automática; possuem limitação a conexões simultâneas e quantidade máxima de dispositivos; e a AnyDesk não possui suporte no Brasil possui limitação a conexões simultâneas e quantidade máxima de dispositivos. Pelos motivos apresentados, este cenário não é recomendado para atender as necessidades do MCOM.

11. Análise comparativa de custos (TCO)

11.1 Solução C – Contratação de solução de mercado (software proprietário

11.1.1 A contratação de nova solução foi a alternativa considerada viável.

11.1.2 Em consulta ao Painel de Preços e Comprasnet, identificou-se que existem contratações na Administração Pública, de soluções de gestão de acesso lógico privilegiado, cujos resultado foi sintetizado na tabela a seguir:

ID	Objeto	Órgão	UASG	Pregão
1	Solução de gerenciamento de acesso lógico privilegiado, contemplando garantia de atualizações de versões e serviços correlatos (12 meses)	ANTT	393001	22/2022
2	Fornecimento de solução de Gerenciamento de Acesso Lógico contemplando serviços técnicos de instalação, configuração, suporte, operação assistida e transferência de conhecimento.	Banco da Amazônia	179007	45/2017
3	Contratação de empresa especializada para o fornecimento de solução de gerenciamento de acesso lógico privilegiado, contemplando garantia de atualização de versões e serviços correlatos	Metro-DF	925046	02/2023

11.1.3 Da análise dos editais e anexos, identificou-se que as contratações possuem similaridade com o que se pretende contratar para o MCOM, embora possuam prazos de contratação (12 e 36 meses) e unidades dos itens com quantitativos diversos (usuários, dispositivos, serviço mensal).

11.1.4 Além disso, observou-se que seus objetos são semelhantes e podem ser consolidados objetivamente entre si na: a) Aquisição de soluções de gestão/gerenciamento de Acesso lógico privilegiado (fornecimento de licenças de software – “subscrição” ou “” - quantificado pela unidade “usuário”, “dispositivo” ou por apenas “solução”) podendo incluir os seguintes serviços agregados: b) Serviços de instalação (quantificados pela unidade serviço); c) Serviços de operação assistida (quantificado pela unidade serviço ou unidade de projeto); d) Serviço de capacitação (quantificado pela unidade turma); e) Serviço de suporte técnico e atualizações de versões (quantificado pela unidade serviço mensal); f) Serviço técnico especializado (quantificado pela unidade horas).

11.1.5 Em resumo, os estudos e pesquisas realizadas consolidam a análise de atendimento dos requisitos, por meio da qual é possível constatar que a Solução C – Contratação de solução de mercado (software proprietário) – é a única que atende integralmente a 100% dos requisitos da contratação pretendida.

11.1.6 Pelos motivos apresentados, este cenário é o recomendado para atender as necessidades do MCOM.

11.1.7 Dessa forma, após a análise comparativa das soluções levantadas e a busca pelo modelo de contratação que melhor atenda e se adeque às necessidades do Ministério, conclui-se pela viabilidade da solução C.

11.1.8 O levantamento de custos se baseou em valores de contratações similares de certames realizados no âmbito da Administração Pública, utilizando Painel de Preços/Comprasnet e consulta ao mercado fornecedor. Dessa forma, seguem os custos totais de propriedade, na forma da tabela abaixo:

Tabela A - Análise consulta painel de preços/comprasnet/Administração Pública

PREGÃO	ORGÃO	UASG	ANÁLISE
PE nº 22/2022	Agência Nacional de Transportes Terrestres	393001	Similar à contratação do MCOM
PE nº 04/202	Banco da Amazônia	179007	Similar à contratação do MCOM

PE nº 02/2023	Companhia Metropolitano do Distrito Federal	925046	Similar à contratação do MCOM

Tabela B - Cálculo dos custos totais estimados de propriedade para um período de 5 (cinco) anos

Item	Descrição	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	Total 5 anos
1	Subscrição anual da solução para atendente com garantia de atualização de versões – para suporte remoto de até 10 usuários simultâneos	198.777,77	198.777,77	198.777,77	198.777,77	198.777,77	**993.888,85**
2	Subscrição anual da solução para dispositivo, com garantia de atualização de versões – para acesso ao ambiente de produção para até 400 dispositivos	507.072,00	507.072,00	507.072,00	507.072,00	507.072,00	**2.535.360,00**
3	Serviço de suporte técnico com operação assistida.	216.266,67	216.266,67	216.266,67	216.266,67	216.266,67	**1.081.333,35**
4	Treinamento (Turma de 5 alunos)	10.000,00	-	-	-	-	**10.000,00**
	VALOR TOTAL	**932.116,44**	**922.116,44**	**922.116,44**	**922.116,44**	**922.116,44**	**4.620.582,20**

12. Descrição da solução de TIC a ser contratada

12.1 O detalhamento técnico final da solução encontra-se descrito no ANEXO I, deste Estudo Técnico.

13. Estimativa de custo total da contratação

Valor (R$): 932.116,44

13.1 De forma preliminar, estima-se para esta contratação o valor de R$ 932.116,44 (novecentos e trinta e dois mil cento e dezesseis reais e quarenta e quatro centavos) que deverá ser atualizado mediante Relatório de Pesquisa de Preço, artefato que compõe o processo de contratações de TIC;

13.2 A estimativa preliminar dos custos da contratação foi formulada considerando as diretrizes da Instrução Normativa SEGES nº 65, de 7 de julho de 2021, bem como as disposições pertinentes às soluções de Tecnologia da Informação e Comunicação descritas na IN SGD /ME nº 94 /2022, juntamente com suas atualizações. A memória de cálculo correspondente encontra-se anexada a este Estudo Técnico Preliminar da Contratação.

14. Justificativa técnica da escolha da solução

14.1 Do ponto de vista técnico, observa-se ao longo do estudo técnico que, dentre as três soluções analisadas, a **Solução C – Contratar solução de mercado específica para gerenciamento de acesso lógico privilegiado,** contemplando garantia de versões e serviços correlatos é a única que atende 100% (cem por cento) dos requisitos técnicos provendo todas as funcionalidades e serviços necessários para o Ministério em uma única solução, pois as demais soluções analisadas não atendem os requisitos ou os atendem apenas parcialment

14.2 O agrupamento dos itens do objeto em um grupo único reforçará o objetivo da contratação, que é garantir a segurança das informações no ambiente computacional do Ministério, uma vez que, durante a execução contratual, o MCOM deverá fornecer informações reservadas e outros detalhamentos técnicos sensíveis da infraestrutura de TI do Ministério. Além disso, os itens do objeto dessa contratação guardam compatibilidade, similaridade e dependência entre si e são normalmente comercializados por empresas que os vendem na sua totalidade. Desse modo, considera-se ainda que um único fornecedor para os itens contratados ocasione uma entrega de serviços com resultados superiores ao MCOM caso comparados com serviços executados por empresas diferentes, pois os itens guardam total relacionamento entre si.

15. Justificativa econômica da escolha da solução

15.1 Com base na análise comparativa de custos totais de propriedade (TCO), item 11 deste Estudo Técnico, a equipe concluiu que a Solução C se mostra mais econômica para atender as necessidades do MCOM.

16. Benefícios a serem alcançados com a contratação

16.1 Dentre os principais resultados e benefícios a serem alcançados com a contratação, pode-se destacar:

- Aumentar a segurança e o gerenciamento do uso de credenciais privilegiadas por meio dos acessos remotos no ambiente computacional do MCOM;
- Unificar e padronizar todos os acessos remotos realizados no ambiente computacional do MCOM;
- Criar trilhas de auditoria por meio de logs e gravação de vídeos de toas as ações realizadas durante um atendimento por meio de um acesso remoto, possibilitando auditar as atividades dos acessos remotos ao ambiente de rede do MCOM;
- Garantir a segurança de todas as conexões remotas de forma criptografada e controladas pelo MCOM;

- Otimizar o uso dos recursos humanos para atendimentos de suporte de forma remota em todo o ambiente do MCOM
- Otimizar o tempo de resposta e o SLA dos atendimentos de primeiro nível possibilitando numa mesma sessão remota o acesso de vários atores de forma controlada, segura e com todas as ações gravadas e auditadas;
- Possibilitar escalar chamados quando necessário dentro de uma mesma sessão remota;
- Possibilitar atendimentos remotos para dispositivos móveis smartphones;
- Possibilitar aferir a satisfação dos usuários ao final dos atendimentos de forma automatizada, disponibilizando os logs e vídeos das ações realizadas quando necessário.

17. Providências a serem Adotadas

17.1 Elaboração do Plano de Implantação da solução compreendendo a instalação e configuração do software de Gerenciamento de Acesso Lógico Privilegiado.

17.2 Ministério das Comunicações irá designar equipe para fiscalização e gestão do contrato nos moldes do Art. 29 da IN SGD/ME nº 94/2022.

17.3 A Contratada deverá designar preposto para representar a empresa e atuar como principal interlocutor junto ao MCOM.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

18.1.1 Com base nas informações levantadas ao longo do estudo técnico preliminar, os integrantes requisitante e técnico, da equipe de planejamento, declaram que a contratação de solução de gerenciamento de acesso lógico privilegiado, contemplando garantia de atualizações de versões e serviços correlatos se mostra a mais viável.

18.1.2 Dessa forma, a Solução C - Contratação de nova solução é a opção que se apresenta mais vantajosa, do ponto de vista técnico e econômico, sendo relevante e essencial para o desenvolvimento das atividades e trabalhos realizados pelo MCOM.

18.1.3.Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que recomendamos o prosseguimento da contratação.

18.1.4 O presente Estudo Técnico preliminar da Contratação foi elaborado em harmonia com a Instrução Normativa SGD /ME nº 94/20229, da Secretaria de Governo Digital do Ministério da Economia, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Despacho: Estudo Técnico Preliminar elaborado em conformidade com a Instrução Normativa SGD/ME nº 94/2022. Assim, declaro adequada, do ponto de vista técnico, a contratação da solução elencada neste documento.

MICHEL GULARTE RECONDO

Integrante Técnico

Assinou eletronicamente em 08/11/2023 às 14:43:46.

Despacho: Estudo Técnico Preliminar elaborado em conformidade com a Instrução Normativa SGD/ME nº 94/2022. Assim, declaro adequada, do ponto de vista negocial, a contratação da solução elencada neste documento.

VICTOR HENRIQUE HISAO TAIRA

Integrante Requisitante

Assinou eletronicamente em 10/11/2023 às 10:41:12.

Despacho: Aprovo o presente Estudo Técnico Preliminar e reconheço a adequação, do ponto de vista técnico, da contratação da solução descrita no documento.

HELDER MOTA GOMES

Autoridade Máxima de TIC

Assinou eletronicamente em 08/11/2023 às 17:27:30.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - GALP_ANEXO I DO ETP - REQUISITOS TÉCNICOS.pdf (242.11 KB)
- Anexo II - GALP_ANEXO II DO ETP - PESQUISA DE PREÇO PRELIMINAR.pdf (299.25 KB)

ANEXO I DO ETP – REQUISITOS TÉCNICOS OBRIGATÓRIOS DA SOLUÇÃO

GERENCIAMENTO DE ACESSO LÓGICO PRIVILEGIADO

1. SUBSCRIÇÃO ANUAL DA SOLUÇÃO – ATENDENTE

1.1. O licenciamento deverá contemplar 10 (dez) atendentes simultâneos para até 1.290 dispositivos (estações de trabalho).

1.2. Possibilidade de iniciar sessão de suporte via portal web ou através de um ícone no computador do cliente, selecionando entre as opções: clicando no nome do Atendente, informando uma chave de sessão, ou escolhendo uma categoria de problemas.

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

1.4. Possibilidade de iniciar sessão de suporte através de ícone no desktop e selecionando o nome do Atendente, informando uma chave de sessão, ou escolhendo uma categoria de problemas.

1.5. Possibilidade de iniciar a sessão através da console informando IP ou hostname do equipamento.

1.6. A solução não deve exigir a necessidade de instalação prévia de componente cliente nos equipamentos da rede. O cliente deve ser instalado no momento da sessão e desinstalado após a 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 atendente precise elevar os privilégios da sessão e não possua a credencial necessária.

1.9. Solução deve suportar a injeção automática de senhas, permitindo que os usuários autentiquem 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. Permitir iniciar sessão com compartilhamento de tela limitado ou completo.

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

1.12. Permitir utilização de comando Shell em uma seção com scripts pré-preparados, sem que os scripts precisem estar ou serem copiados para o equipamento do usuário.

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

1.14. Permitir visualização da informação do sistema do cliente com as seguintes informações: hardware, disco, processos, event logs, interfaces de rede, softwares instalados, patchs de sistema operacional, tarefas agendadas.

1.15. Permitir chat entre representante e usuário.

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

1.17. Permitir reiniciar o Windows do cliente voltando à sessão automaticamente;

1.18. Permitir iniciar sessão SSH ou telnet.

1.19. Permitir customizar o portal de suporte, o componente cliente e o ícone distribuído aos clientes (banner, cor, informações).

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 o uso da Tecnologia Intel Active Management, para que os usuários com privilégios possam oferecer suporte a sistemas Windows totalmente provisionados da Intel® vPro abaixo do nível do Sistema Operacional, independentemente do status ou estado de energia desses sistemas remotos.

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 membroda 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 outro representante 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. Permitir transferir a sessão com outro representante ou outra equipe.

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 X;
- **c)** Sistemas operacionais Linux;

d) Sistemas operacionais ChromeOS;

e) Dispositivos móveis;

f) Apple Ios;

g) Android;

h) BlackBerry;

i)Windows Mobile;

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 em 32 e 64 Bit, Sistemas Operacionais Mac e também Sistemas operacionais Linux em 32 ou 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. O vídeo do atendimento deve demonstrar qual parte (atendente ou usuário) estava no controle do teclado e do mouse a todo o momento.

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 ferramentas autenticação de dois fatores, usando uma senha única baseada em tempo (TOTP). Suportando soluções como: Google Authenticator, Authy, YubioAth Desktop, GAuth Authenticator, 1Password e etc;
- **c)** Deve ser possível a utilização de SmartCard para autenticação do representantede suporte;
- **d)** A solução deve suportar autenticação física, como por exemplo por "TouchID";
- **e)** Possuir integração com Ferramentas de ITSM, para integrar solução de suporte remoto com solução de gerenciamento de incidentes. Suportando no mínimo a integração com soluções como: Autotask, BMC FootPrints 11 e 12, BMC Remedy, BMC Remedyforce, CA Service Desk, HEAT, JIRA, ServiceNow e Zendesk;
- **f)** Possuir API aberta para construção de outras integrações;

1.50. Possibilitar alterar esquema de cores da resolução até branco e preto, para menor utilização de banda de rede.

1.51. Ser compatível com firewall e ambientes de DMZ para permitir acesso a usuáriose 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 habilitar a gravação automática das sessões de compartilhamento de tela e linha de comando.

1.55. Deve permitir que os representantes de suporte possam "acordar" os dispositivos clientes registrados por meio da tecnologia "Wake-On-Lan".

1.56. Deve permitir que o representante de suporte reinicialize o dispositivo remoto e

após a reinicialização, a sessão seja reestabelecida automaticamente sem a necessidade de iniciar outra sessão.

1.57. Deve ser capaz de se comunicar de forma "peer-to-peer" para sessões de compartilhamento de tela, transferência de arquivos ou shell remoto. Caso naquele momento a solução não consiga conectar de forma "peer-to-peer", a solução deve criar uma conexão se utilizando da console de origem como intermediária.

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

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

1.60. Deve permitir a edição, visualização, deleção e edição de chaves no registro do Windows sem a necessidade de compartilhar a tela do sistema destino.

2. SUBSCRIÇÃO ANUAL DA SOLUÇÃO – DISPOSITIVO

2.1. O licenciamento deverá contemplar 400 (quatrocentos) dispositivos independente da quantidade de usuários privilegiados que necessitem acessar o ambiente de produção.

2.2. A solução deve evitar o uso de protocolos de comunicação legados necessários para acesso, dando preferência a um protocolo totalmente criptografado, como por exemplo TLS 1.2.

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 o acesso a dispositivos de rede como roteadores, switches e outros dispositivos via SSH e Telnet. Este acesso deve ser feito de forma local, sem que haja a necessidade de trafegar estes protocolos em redes inseguras.

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

2.6.1. Uma console instalada diretamente no Sistema Operacional do cliente, que deve suportar Sistemas Operacionais Windows em 32 e 64 Bit, Sistemas Operacionais Mac e também Sistemas operacionais Linux em 32 ou 64Bit.

2.7. 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.

2.8. 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 ferramentas autenticação de dois fatores, usando uma senha única baseada em tempo (TOTP). Suportando soluções como: Google Authenticator, Authy, YubioAth Desktop, GAuth Authenticator, 1Password e etc.

c) A solução deve suportar autenticação fisica, como por exemplo por “TouchID”.

d) A solução deve suportar logon único (SSO), comunicando-se com um provedor de identidade usando SAML 2.0.

e) A solução deve suportar o uso de um certificado válido assinado por CA que valida seu novo o endereço de acesso a ferramenta ou suportar o uso da autoridade certificadora grátis "Let's Encrypt" para obter um certificado.

2.9. 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 definação 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 encerramentoda sessão. Forçando a sessão a se desconectar no horário final agendado. Nessecaso, o usuário deve receber notificações antes de ser desconectado.

c) Notificar destinatários quando uma sessão é iniciada. Suportando no mínimo

uma notificação por e-mail a destinatários designados sempre que uma sessão é iniciada com qualquer ativo.

d) Notificar destinatários quando uma sessão é terminada. Suportando no mínimo uma notificação por e-mail a destinatários designados sempre que uma sessãoé encerrada com qualquer ativo.

e) Exigir aprovação antes do início de uma sessão, suportando no mínimo uma notificação por e-mail de aprovação enviado aos destinatários designadossempre que uma tentativa de sessão com qualquer ativo. Solicitando que o usuário insira um motivo da solicitação, a hora e a duração da solicitação.

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

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

2.12. A solução deve permitir o monitoramento ao vivo das sessões de acesso, etambém deve permitir que os administradores encerrem sessões em andamento se necessário.

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

2.14. A solução deve ser capaz de controlar quais aplicativos podem ser usados por um operador na sessão, limitando o acesso a aplicativos especificados no sistema remoto, permitindo somente os executáveis listados (whitelist) ou negando apenas os executáveis listados (blacklist). Deve ser possível também optar por permitir ou negar oacesso à área de trabalho.

2.15. 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.

2.16. 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".

2.17. Ao acessar um ativo baseado em Linux, injeção de credenciais deve suportar sua

utilização em conjunto com o SUDO.

2.18. A solução deve suportar o acesso a desktops, servidores e outros sistemas remotos autônomos. 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)** Acesso através de cliente de proxy local, que permite o acesso a sistemas Windows autônomos em uma rede, sem cliente pré-instalado.
- **c)** Acesso via cliente de proxy para acessar sistemas em uma rede remota que não tenha uma conexão de internet nativa.
- **d)** Integração com RDP (Remote Desktop Protocol) da Microsoft para realizar sessões utilizando protocolo RDP. Permitindo que os usuários colaborem em sessões e estas sessões possam ser auditadas e gravadas automaticamente.
- **e)** Acesso a dispositivos de rede habilitados para SSH/telnet através de um cliente de proxy efetuando a conexão localmente.
- **f)** Acesso a servidores VNC onde os usuários podem colaborar em sessões e ter as sessões auditadas e gravadas automaticamente.
- **g)** Acesso a páginas Web a partir de agente de proxy local, onde os usuários receberão apenas uma conexão a uma página Web local em uma sessãoauditada e gravada.
- **h)** Túnel de protocolos que permitem estender os recursos de conectividade e auditoria remotas de aplicativos proprietários e/ou de terceiros, como sistemasde controle de integração ou ferramentas de banco de dados personalizadas sem necessidade de VPN.

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

2.20. 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.

2.21. A solução deve ligar ou ativar remotamente máquinas configuradas com a featurede Wake-on-Lan (WOL). Para que se caso a máquina esteja desligada, ainda exista a

possibilidade de conectar-se de forma remota.

2.22. A solução deve permitir que os usuários transfiram arquivos da máquina em que está conectado para o sistema remoto, através da console da solução e sem necessidadede uso de ferramentas de terceiros.

2.23. 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.

2.24. Em caso de colaboração de administradores em uma mesma sessão, a solução deve oferecer chat entre usuários através da mesma console da conexão.

2.25. A solução deve oferecer aos representantes conectados a capacidade de ver informações do sistema sem que seja necessário ter acesso a console do ativo.

2.26. 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.

2.27. 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.

2.28. A solução deve oferecer uma opção de guardar os scripts comuns utilizados pelos administradores como uma opção na console de acesso, permitindo que os administradores executem estes scripts através de um menu de opções.

2.29. A solução deve permitir que os usuários acessem e editem o registro do Windows de forma remota, sem precisar do compartilhamento de tela.

2.30. 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.

2.31. A solução deve conter contar com função que permite agrupar usuários em

equipes permitindo a atribuição de líderes a estes grupos de usuários. Um líder ou gerente de equipe pode monitorar membros da equipe da qual é líder, e opcionalmente pode optar por participar ou assumir as sessões de um membro de sua equipe.

2.32. Solução deve possuir relatórios das sessões de acesso, onde seja possível visualizar todas as sessões, e detalhes destas sessões que incluem informações básicas da sessão, detalhes da sessão, transcrições de bate-papo e gravações em vídeo de compartilhamento de tela, shells de comando e utilização de túnel de protocolos.

2.33. A solução deve possuir relatórios da sessão detalhados que possuam um registro da transcrição completa do bate-papo, o número de arquivos transferidos e ações específicas que ocorreram durante a sessão. Devem contar também com eventos do Windows que apresentam alterações visuais óbvias em uma sessão, incluindo principalmente alterações nas janelas em primeiro plano, contendo o nome do executável e o título da janela.

2.34. 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.

2.35. A solução deve apresentar em relatório as sessões que possuem a gravação ativada, uma opção para reprodução de vídeo de sessões individuais.

2.36. Caso o usuário utilize a opção de túnel de sessão, deve ser possível visualizar as gravações de vídeo da área de trabalho inteira do usuário.

2.37. 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.

2.38. 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 aduração média das sessões.

2.39. A solução deve possuir relatórios de atividades das equipes, que devem conter informações sobre os usuários conforme eles entram ou saem do console de acesso da ferramenta, assim como mensagens de bate-papo enviadas entre membros da equipe, ações de compartilhamento de tela de usuário para usuário e arquivos compartilhados

e baixados.

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

2.41. 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 acionamentoem nível de resolução de problemas pelo próprio fabricante se necessário, alémdo nível de suporte que deverá ser prestado pela Contratada em conjunto, conforme previsto no Caderno de Cotação e seus apêndices.

ANEXO II DO ETP - PESQUISA DE PREÇO PRELIMINAR

GERENCIAMENTO DE ACESSO LÓGICO PRIVILEGIADO

INCISO II – CONTRATAÇÕES SIMILARES

ITEM 1 - SUBSCRIÇÃO ANUAL DA SOLUÇÃO PARA ATENDENTE, COM GARANTIA DE ATUALIZAÇÃO DE VERSÕES – PARA SUPORTE REMOTO DE ATÉ 10 USUÁRIOS SIMULTÂNEOS

- **UASG 393001- Agência Nacional de Transportes Terrestres - Pregão Eletrônico n° 22/2022**

Descrição: Contratação de solução de tecnologia da informação e comunicação de gerenciamento de acesso lógico privilegiado, contemplando garantia de atualizações de versões e serviços correlatos,

Data: 27/12/2022.

Item	Descrição	Unidade de Medida	Quant	Val. Unit	Val. Total
1	Subscrição anual da solução para atendente, com garantia de atualização de versões – para suporte remoto de até 10 usuários	Usuários	1	247.000,00	247.000,00

Para fins de comparação de custos, foi realizada a extração do valor unitário da contratação da ANTT. A seguir, o demonstrativo:

Valor unitário para 12 meses
R$ 247.000,00

- **UASG 179007 – Banco da Amazônia - Pregão Eletrônico n° 04/2023**

Descrição: Contratação de empresa especializada para manutenção e expansão do licenciamento de solução de gerenciamento de acesso lógico, contemplando serviços técnicos de suporte com operação assistida e transferência de conhecimento

Data: 03/03/2023

Categoria	Descrição	Unidade de Medida	Quant.	Valor Unitário (R$)	Valor Total (R$)
Item 2 - Expansão do licenciamento da solução de gerenciamento de acesso lógico para o atendimento remoto criptografado e privilegiado a estações de trabalho pelo período de 12 (doze) meses.	Serviço anual de subscrição da solução de gerenciamento de acesso lógico para atendimento remoto criptografado e privilegiado a estações de trabalho pelo período de 12 (doze) meses.	Usuários	10	16.700,00	167.000,00

Para fins de comparação de custos, foi realizada a extração do valor total relativo a 10 usuários, que é a quantidade única do item previsto para o MCOM, qual seja: ***Subscrição anual da solução para ATENDENTE, com garantia de atualização de versões – para suporte remoto de até 10 usuários simultâneos.***

Assim sendo, a quantidade "1" da tabela do MCOM corresponde à quantidade "10" do Pregão do BASA. Abaixo, o demonstrativo do cálculo realizado:

Valor total para 10 usuários por 12 meses (10*16.700,00) - BASA	Valor total para solução que atenda 10 usuários, por 12 meses - MCOM
R$ 167.000,00	R$ 167.000,00

- **UASG 926046 – Companhia Metropolitano do Distrito Federal - Pregão Eletrônico n° 02/2023**

Descrição: Contratação de empresa especializada para o fornecimento de solução de gerenciamento de acesso lógico privilegiado, contemplando garantia de atualização de versões e serviços correlatos.

Data: 04/05/2023

Descrição	Unidade de Medida	Prazo	Quant.	Valor Unitário (R$)	Valor Total (R$)
Item 1 – Serviço de subscrição da solução para atendimento de suporte remoto aos usuários finais	Usuários	36 meses	5	54.700,00	273.500,00

Para fins de comparação de custos, foi realizada a extração do valor unitário relativo a 36 meses, dividido por 3, para a obtenção do valor relativo a 12 meses. Abaixo, o demonstrativo do cálculo realizado:

Valor unitário, por atendente/usuário para 36 meses	Valor unitário, por atendente/usuário para 12 meses **54.700,00 / 3**	Valor unitário, por 10 atendentes/usuários para 12 meses **10 *** 18.233,33
R$ 54.700,00	R$ 18.233,33	**R$** 182.333,30

ITEM 2 - SUBSCRIÇÃO ANUAL DA SOLUÇÃO PARA DISPOSITIVO, COM GARANTIA DE ATUALIZAÇÃO DE VERSÕES – PARA ACESSO AO AMBIENTE DE PRODUÇÃO PARA ATÉ 400 DISPOSITIVOS INDEPENDENTE DA QUANTIDADE DE USUÁRIOS SIMULTÂNEOS.

- **UASG 393001- Agência Nacional de Transportes Terrestres - Pregão Eletrônico n° 22/2022**

Item	Descrição	Unidade de Medida	Quant	Val. Unit	Val. Total
2	Subscrição anual da solução para dispositivo,com garantia de atualização de versões – para acesso ao ambiente de produção para até 3.500 dispositivos.	Dispositivos	1	3.100.000,00	3.100.000,00

Para fins de comparação de custos, foi realizada a extração do valor unitário relativo a 3.500 dispositivos; calculado o valor de 1 dispositivo e multiplicado pela quantidade de 400 dispositivos para o Ministério. Abaixo, o demonstrativo do cálculo realizado:

Valor para 3.500 dispositivos	Valor para 1 dispositivo **3.100.000 / 3.500**	Valor para 400 dispositivos **400 * 885,71**
R$ 3.100.000,00	R$ 885,71	**R$ 354.284,00**

- **UASG 179007 – Banco da Amazônia - Pregão Eletrônico n° 04/2023**

Categoria	Descrição	Unidade de Medida	Quant.	Valor Unitário (R$)	Valor Total (R$)
Item 3 - Expansão do licenciamento da solução de gerenciamento de acesso lógico para o acesso remoto criptografado e privilegiado ao ambiente de produção pelo período de 12 (doze) meses.	Serviço anual de subscrição da solução de gerenciamento de acesso lógico para acesso remoto criptografado e privilegiado ao ambiente de produção do BASA pelo período de 12 (doze) meses.	Unidades de Dispositivo	500	894,00	447.000,00

Para fins de comparação de custos, foi realizada a extração do valor unitário da contratação do BASA e multiplicado pelo quantitativo de 400 estimado para o MCOM. Abaixo, o demonstrativo do cálculo realizado:

Valor unitário para 12 meses	**Valor unitário para 12 meses – MCOM** **400 * 894,00**
R$ 894,00	**R$ 357.600,00**

- **UASG 926046 – Companhia Metropolitano do Distrito Federal - Pregão Eletrônico n° 02/2023**

Descrição	Unidade de Medida	Prazo	Quant.	Valor Unitário (R$)	Valor Total (R$)
Item 2 – Serviço de subscrição da solução para acesso lógico privilegiado ao ambiente de produção	Dispositivos	36 meses	300	6.070,00	1.821.000,00

Para fins de comparação de custos, foi realizada a extração do valor unitário relativo a 36 meses, dividido por 3, para a obtenção do valor relativo a 12 meses. Abaixo, o demonstrativo do cálculo realizado:

Valor unitário, por dispositivo, para 36 meses	**Valor unitário, por dispositivo, para 12 meses** **6.070,00 / 3**	**Valor para 400 dispositivos** **400 * 2.023,33**
R$ 6.070,00	R$ 2.023,33	**R$ 809.332,00**

ITEM 3 - SERVIÇO DE SUPORTE TÉCNICO COM OPERAÇÃO ASSISTIDA.

- **UASG 393001- Agência Nacional de Transportes Terrestres - Pregão Eletrônico n° 22/2022**

Item	Descrição	Unidade de Medida	Quant	Val. Unit	Val. Total
3	Serviço de suporte técnico com operação assistida.	Serviço Mensal	12	11.666,66	140.000,00

Para suporte técnico e operação assistida, o valor a ser comparado é o mesmo do pregão da ANTT, conforme abaixo:

Valor unitário mensal	Valor total para 12 meses
R$ 11.666,66	R$ 140.000,00

- **UASG 179007 – Banco da Amazônia - Pregão Eletrônico n° 04/2023**

Categoria	Descrição	Unidade de Medida	Quant.	Valor Unitário (R$)	Valor Total (R$)
Item 4 - Suporte Técnico com operação assistida e transferência de conhecimento para a solução pelo período de 12 (doze) meses.	Serviço de Suporte Técnico com operação assistida e transferência de conhecimento da solução pelo período de 12 (doze)meses.	Serviço Mensal	12	19.700,00	236.400,00

Para suporte técnico e operação assistida, o valor a ser comparado é o mesmo do pregão do BASA, conforme abaixo:

Valor unitário mensal	Valor total para 12 meses
R$ 19.700,00	R$ 236.400,00

- **UASG 926046 – Companhia Metropolitano do Distrito Federal - Pregão Eletrônico n° 02/2023**

Descrição	Unidade de Medida	Prazo	Quant.	Valor Unitário (R$)	Valor Total (R$)
Item 3 – Serviço de suporte técnico com operação assistida e transferência de conhecimento para o Lote 1.	Serviço Mensal	36 meses	36	22.700,00	817.200,00

Para suporte técnico e operação assistida, o valor a ser comparado é o mesmo do pregão do Metrô-DF, conforme abaixo:

Valor unitário mensal	Valor total para 12 meses
R$ 22.700,00	R$ 272.400,00

ITEM 4 - TREINAMENTO (TURMA DE 5 ALUNOS)

- **UASG 393001- Agência Nacional de Transportes Terrestres - Pregão Eletrônico n° 22/2022**

Item	Descrição	Unidade de Medida	Quant	Val. Unit	Val. Total
4	Treinamento (Turma de 5 alunos)	Turma	1	10.000,00	10.000,00

Para Treinamento, o valor a ser comparado é o mesmo do pregão da ANTT, conforme abaixo:

Valor unitário por turma	Valor total para 1 turma
R$ 10.000,00	R$ 10.000,00

QUADRO RESUMO DEMONSTRATIVO DOS VALORES MÉDIOS ESTIMADOS, OBTIDOS NA PESQUISA EM CONTRATAÇÕES PÚBLICAS

Item	Descrição	Unidade de Medida	Quantidade	CONTRATAÇÕES SIMILARES NA ADMINISTRAÇÃO PÚBLICA			Val. Unit (Média)	Val. Total (Média)
				ANTT UASG: 393001 PE 22/2022	BASA UASG: 179007 PE 04/2023	METRÔ-DF UASG: 926046 PE 02/2023		
				Val. Unit	Val. Unit	Val. Unit		
1	Subscrição anual da solução para atendente, com garantia de atualização de versões – para suporte remoto de até 10 usuários simultâneos	Usuários	1	247.000,00	167.000,00	182.333,30	198.777,77	198.777,77
2	Subscrição anual da solução para dispositivo, com garantia de atualização de versões – para acesso ao ambiente de produção para até 400 dispositivos	Dispositivos	1	354.284,00	357.600,00	809.332,00	507.072,00	507.072,00
3	Serviço de suporte técnico com operação assistida.	Serviço Mensal	12	140.000,00	236.400,00	272.400,00	216.266,67	216.266,67
4	Treinamento (Turma de 5 alunos)	Turma	1	10.000,00	-	-	10.000,00	10.000,00
VALOR TOTAL ESTIMADO							**R$ 932.116,43**	