FORMULÁRIO DE PARTICIPAÇÃO PARA COLETA DE PREÇOS – 09/2022
1. Parte Contratante
Razão Social: **FUNDAÇÃO INSTITUTO DE PESQUISA E ESTUDO DE DIAGNÓSTICO POR IMAGEM – FIDI**
Sede: Av. Paulista, 2537 10 andar Bela Vista, São Paulo – SP, 01311-300
2. Preâmbulo
A Fundação Instituto de Pesquisa e Estudo de Diagnóstico por Imagem torna pública a realização de Coleta de Preços, pelo critério de menor custo e escopo aderente a necessidade da FIDI, objetivando a contratação de software para Gerenciamento de Acesso Privilegiado (PAM) para proteção de credenciais privilegiadas e automação do processo de acesso em formato SAAS (Software como serviço), com a prestação de serviços de implantação, treinamento, suporte técnico, manutenções corretivas e preventiva e customização, bem como demais serviços, sendo as condições fixadas na presente Coleta de Preços.
3. Prazo para envio das Propostas
As propostas deverão ser enviadas nos e-mails informados no contato até o dia **22.07.2022**
4. Objeto da Coleta de Preços
As informações com relação as especificações técnicas necessárias ao objeto deste instrumento, para participação nessa convocação, estão descritas no **Anexo I**, **II** e **III** que deverão ser detalhadas na proposta comercial encaminhada pelo participante, onde elas serão analisadas e havendo necessidade, serão discutidas via e-mail para melhor entendimento e/ou esclarecimento da necessidade.
5. Contato FIDI
Esclarecimentos relativos a presente Coleta de Preços serão prestados quando solicitados à FIDI no setor de Suprimentos através dos contatos abaixo: Josiane Santos através do e-mail josiane.nsantos@fidi.org.br Fambber Ribeiro através do e-mail fambber.ribeiro@fidi.org.br Elaine Gomes através do e-mail elaine.gomes@fidi.org.br Ou através do telefone (11) 5088-7900 Sede São Paulo
6. Prazo de vigência Contratual

O vínculo será contratual de até 12 meses de duração, podendo ser renovado por mais até no máximo 24 meses mediante negociação entre ambas as partes e investimento demandado pela Parte Interessada para o Projeto.

7. Critérios de Participação

As propostas apresentadas serão julgadas e classificadas, sendo verificada sua conformidade com os critérios abaixo:

a) Adequação das propostas ao objeto e critérios de especificação conforme **Anexo I, Anexo II e Anexo III** da coleta de preços;

b) Melhor aderência ao processo, política, necessidades e determinações da área responsável na FIDI que utilizará os serviços;

c) Integrações com plataformas de sistemas operacionais ou ERP's, caso necessário;

d) Qualidade e eficiência do funcionamento da ferramenta, sendo medida através de apresentação e relatórios, caso necessário;

e) Preço;

f) Condição de pagamento aderente a nossa política de pagamento;

g) Suporte técnico e o prazo de sla proposto para os atendimentos.

8. Anexos

Anexo I – Termo de Referência Especificações técnicas da prestação de serviços e base da tomada.

Anexo II- SLA de Atendimento

Anexo III– Relação de Unidades de Atendimento e dados para Faturamento

9. Prazo e forma de entrega

A disponibilização dos serviços deverão ser conforme indicado nas informações do Anexo I, assim como negociações e acordos comerciais, sendo o prazo de entrega em torno do que for alinhado entre as partes, somente podendo sofrer alteração uma vez acordado e formalizado entre as mesmas, após o envio da confirmação de compra sendo esta via aceite de proposta e/ou minuta contratual através de e-mail e/ou via física.

10. Condições Adicionais

Os locais de implantação dos serviços ofertados e faturamento serão determinados conforme demandas encaminhadas através de pedidos de compra conforme CNPJ's informados no Anexo III, uma vez alinhada com a área responsável, havendo necessidade o faturamento somente será aprovado mediante aprovação de relatório de faturamento que deverá ser emitido pelo prestador de serviços.

1. CONDIÇÕES DE PARTICIPAÇÃO NA COLETA DE PREÇOS

1.1. Poderão participar da presente Coleta todos os interessados no ramo pertinente ao objeto cotado, que apresentarem propostas até a data limite estipulada.

1.2. Na presente seleção é vedada a participação de empresas em processo de consórcio.

1.3. A participação na presente seleção implica na aceitação integral de todos os termos desta Coleta.

1.4 O vencedor da presente Coleta de preços terá vínculo com a FIDI através de contrato de prestação de serviços, onde serão firmados os direitos e deveres de ambas as partes e as condições comerciais de fornecimento.

1.5 As empresas deveram enviar anexo a proposta o cartão de CNPJ.

1.6 As empresas deveram enviar as propostas em papel timbrado e com todas as condições descritas na coleta.

2. DIVULGAÇÃO DO VENCEDOR E DOCUMENTAÇÃO REFERENTE À HABILITAÇÃO JURÍDICA

2.1. A divulgação do vencedor será efetuada no site da FIDI, para que todos os participantes tomem conhecimento.

2.2. A documentação de habilitação do fornecedor que apresentar a proposta vencedora deverá ser enviada para os e-mails informados no formulário de participação desta coleta no prazo de até 02 dias úteis após a solicitação, contendo:

- Registro comercial, no caso de empresa individual;

- RG do representante legal da pessoa jurídica;

- Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, acompanhando, se for o caso, dos documentos de eleição de seus administradores;

- Inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

- Certidão Negativa de Débitos de Tributos Federais;

- Certidão Negativa de Débitos de Tributos Estaduais;

- Certidão Negativa de Débitos de Tributos Municipais;

- Comprovação de regularidade perante a Seguridade Social;

- Comprovação da regularidade perante o Fundo de Garantia do Tempo de Serviço – FGTS (emitido pela Caixa Econômica Federal – CEF, no site www.caixa.gov.br);

- Comprovação da autorização de funcionamento emitida pela ANVISA (original ou cópia autenticada) e cópia autenticada do Alvará Sanitário ou da Licença de funcionamento do fornecedor, expedido pelo Serviço de Vigilância Sanitária, em vigência, conforme Código Sanitário e Leis complementares. Não será aceito protocolo de alvará (ou licença) inicial ou de renovação; **(Quando Aplicável)**

- Em caso de empresa ou representante exclusivo, apresentar declaração original ou autenticada vigente com a data de validade expressa no documento e em papel timbrado do fabricante, que comprove que o fornecedor está credenciado pelo mesmo para comercializar o produto de sua marca cotado. Caso esta autorização não tenha validade por toda a vigência do contrato, apresentar documento complementar de atualização do prazo emitido pelo fabricante dos produtos ofertados; **(Quando aplicável)**

- Apresentar, quando solicitado, documento comprobatório do registro vigente no Ministério da Saúde (identificando o item em cada registro em sua proposta), através de:

I - Publicação do registro no DOU (Diário Oficial da União); **(Quando Aplicável)**

II - Comprovante de registro emitido pelo Ministério da Saúde demonstrando sua vigência, caso a validade do registro esteja vencida, apresentar também o pedido de revalidação datado do semestre anterior ao vencimento do registro, acompanhado do registro vencido. **(Quando Aplicável)**

3. PROCEDIMENTOS PARA JULGAMENTO

3.1. Após o encerramento da coleta de preços pelo site, não será permitida qualquer alteração em seu conteúdo que possa influenciar no julgamento final, nem admitido à Seleção qualquer proponente retardatário.

3.2. Será considerada a melhor proposta a que resultar em menor custo para a FIDI, sendo este calculado pela verificação e comparação dos critérios estipulados no item 7 do Formulário para Participação da Coleta de Preços.

3.3. Finalizado o procedimento de Coleta de Preços, o Gerente de Suprimentos deverá aprovar a melhor proposta apurada junto ao departamento da FIDI solicitante e em casos específicos submeter ao Comitê de Compras formados por membros da FIDI.

3.4. Escolhida a proposta vencedora, o interessado será informado via e-mail para que apresente a documentação referida na cláusula 2.2 desta coleta de preços além da divulgação no site da FIDI.

3.5. Quando nenhum dos participantes atender aos requisitos apresentados na presente Coleta de Preços ou o número de respostas for insuficiente para a análise do processo conforme o tipo de serviço ou produto do referido objeto requisitado, a FIDI poderá cancelar a Coleta de Preços publicada através da divulgação via site da FIDI, sendo que:

- A FIDI não poderá vedar a participação de nenhum dos fornecedores correspondentes da Coleta de Preços anterior numa nova publicação caso ocorra;

- A FIDI deverá manter essa publicação de cancelamento divulgada num prazo mínimo de 10 dias antes de partir para uma nova Coleta de Preços referente ao mesmo objeto cotado e cancelado;

4. RECURSOS

4.1. Após a divulgação do vencedor da coleta de preços no site da FIDI, caso algum participante se sinta prejudicado em razão do julgamento das propostas, poderá manifestar, sendo-lhe concedido o prazo de até 03 (três) dias úteis para interpor as razões de recurso após a data de divulgação do vencedor.

4.2. A FIDI decidirá quanto aos recursos, no prazo de até 15 (quinze) dias úteis.

4.3. A interposição de recurso não suspende o julgamento das propostas.

5. CONDIÇÕES DE FORNECIMENTO E FATURAMENTO

5.1. O vencedor deverá fornecer os serviços nos locais e quantidades indicados pela FIDI, no prazo estabelecido no fechamento da compra, sendo de sua inteira responsabilidade os eventuais danos ou prejuízos causados por seus funcionários no momento da entrega.

5.2 Prazo de entrega deverá ocorrer em até 05 dias úteis ou conforme acordado com a área responsável direto nas Unidades Operacionais ou no nosso Centro de Distribuição, cujos endereços estão listados no Anexo II.

5.3. O descumprimento do prazo de entrega estipulado pela FIDI ou a entrega de materiais/serviços fora das especificações, implicarão no pagamento de multa não compensatória diária correspondente a 2% (dois por cento) do valor referente à solicitação de fornecimento não cumprida.

5.4. No caso de reincidência de atrasos na entrega dos serviços, caso seja acordado entregas fracionadas, de no mínimo por 3 (três) vezes, a FIDI poderá cancelar a compra não sendo devido ao Vencedor qualquer valor a título de indenização.

5.5 Deve ser emitida uma nota fiscal por pedido de compra enviado.

5.6. Serão de responsabilidade exclusiva do contratado o recolhimento de todos os tributos incidentes na fabricação/prestação de serviços do objeto desta Coleta de Preços, que for de sua competência.

5.7. A forma de faturamento e pagamento para a FIDI ocorre da seguinte forma:

I) Prestação de serviços para Contratos dos clientes da FIDI dentro do escopo de Gestão

CNPJs (55.401.178/0005-60 / 55.401.178/0010-27)

• Para as notas fiscais e boletos bancários emitidos e enviados até o dia 10 (dez) do mês vigente, sendo estes referentes a prestação de serviços do mês precedente, os pagamentos serão realizados no dia 17 (dezessete) do mês subsequente;

• Para as notas fiscais e boletos bancários emitidos e enviados entre os dias 11 (onze) e 25 (vinte e cinco) do mês vigente, sendo estes referentes a prestação de serviços do mês precedente, o pagamento se dará no dia 25 do mês subsequente.

6. REGRAS E PROCEDIMENTOS DA INSTITUIÇÃO

A seguir regras e procedimentos da nossa Instituição que devem ser aplicados e seguidos durante todo o processo de negociação da Coleta de Preços:

PROPRIEDADE E DIREITO INTELECTUAL

6.1. A FIDI reconhece e concorda que todo e qualquer direito relativo a toda e qualquer marca, patente, modelo industrial, software, segredo de negócio ou comercial, documento, informação, arquivos eletrônicos, direitos autorais, invenções, modelos industriais e qualquer outro bem ou direito que configure ou possa vir a configurar direito de propriedade intelectual ou direito de propriedade industrial ("Propriedade Intelectual") proveniente dos Serviços é de propriedade exclusiva da Parte Participante. Nesse caso, a FIDI deve dar licença gratuita para a Parte Participante das novas Propriedades Intelectuais provenientes dos Serviços.

6.2. A FIDI compromete-se a praticar todos e quaisquer atos convenientes ou necessários a fim de manter efetivas em quaisquer circunstâncias as disposições da Cláusula acima.

6.3. A FIDI reconhece que os Sistemas Operacionais são protegidos pelas leis de direito autoral e, portanto, concorda, por si ou por terceiros, (i) em não copiar, disponibilizar, fornecer, vender, emprestar, transferir ou de qualquer forma alienar qualquer componente dos Sistemas Operacionais, ou ainda decompilar, traduzir, fazer engenharia reversa, copiar códigos-fonte dos Sistemas Operacionais; (ii) usar os Sistemas Operacionais para outro fim além daquele previsto no Contrato Específico; (iii) modificar os Sistemas Operacionais. A FIDI concorda em informar de forma detalhada aos usuários finais dos Sistemas Operacionais as condições e termos do Contrato Específico e exigir e garantir que o usuário final cumpra os mesmos.

6.4. As cessões em regime de comodato dos Sistemas Operacionais são concedidas pelo prazo de vigência previsto pelo Contrato Específico, em caráter não exclusivo, intrasferível.

6.5. A Parte Participante deverá substituir os Sistemas Operacionais por novos modelos com as mesmas especificações técnicas e nas mesmas quantidades a cada 60 (sessenta) meses, em casos de renovações da vigência do Contrato Específico.

6.6. A FIDI reconhece expressamente que a Parte Participante é a proprietária única e exclusiva dos Sistemas Operacionais a serem instalados nas suas dependências, sendo que a FIDI deterá, apenas e tão somente, a posse dos Sistemas Operacionais.

6.7. As estipulações desta Cláusula permanecerão em vigor, mesmo em caso de término do Contrato Específico.

CONFIDENCIALIDADE

6.8. Todas as informações e documentos relacionados ao Contrato Específico ou trocados em virtude de sua celebração por qualquer das Partes ("Parte Divulgadora") para outra(s) Parte(s) ("Parte Receptora") serão considerados e tratados, para todos os fins, como "Informações Confidenciais" e, mesmo após sua divulgação, permanecerão de titularidade exclusiva da Parte Divulgadora.

6.9. A Parte Receptora utilizará as Informações Confidenciais somente para a execução do Contrato Específico, manterá em sigilo todas as Informações Confidenciais e não as divulgará para terceiros. Não obstante o exposto, a Parte Receptora poderá divulgar tais Informações Confidenciais para seus representantes que necessitem ter acesso a tais Informações Confidenciais ao longo da execução de quaisquer das obrigações estabelecidas no Contrato Específico.

6.10. As disposições desta Cláusula não se aplicarão à divulgação de Informações Confidenciais para qualquer autoridade Governamental em virtude das Normas aplicáveis. Neste caso, a Parte Receptora deverá notificar a Parte Divulgadora sobre a determinação de proceder a tal divulgação. Quando aplicável, a Parte Divulgadora terá o direito de tomar as medidas que julgar necessárias para evitar a divulgação das Informações Confidenciais para as referidas autoridades governamentais.

6.11. As Informações Confidenciais não incluem informações que: (a) sejam comumente conhecidas ou disponíveis por publicação, uso comercial, ou por outras formas que não constituam violações das obrigações por parte da Parte Receptora; (b) sejam conhecidas pela Parte Receptora no momento da divulgação e não estejam sujeitas a restrições; (c) sejam legalmente obtidas de um terceiro que tenha o direito de efetuar tal divulgação; ou (d) sejam, por escrito, liberadas pela Parte Divulgadora para publicação.

6.12. Caso a Parte Receptora não esteja segura com relação à caracterização ou não de determinada informação como sendo Informação Confidencial, a Parte Receptora deverá buscar orientação por escrito da Parte Divulgadora antes de divulgar tal informação para terceiros.

6.13. A Parte Receptora responderá pelas perdas e danos que causar à Parte Divulgadora que sejam resultado do descumprimento do disposto nesta Cláusula.

6.14. As disposições desta Cláusula sobreviverão ao término do Contrato Específico por um período de 5 (cinco) anos contados da referida data de término, independente do motivo.

6.15. A Parte Participante declara que acessou, tomou conhecimento e entendeu o teor do Código de Conduta e do Manual de Conduta da Parte Contratante, disponibilizados nos links http://www.fidi.org.br/wp-content/uploads/2015/11/Codigo-de-Conduta-FIDI.pdf e http://www.fidi.org.br/wp-content/uploads/2015/11/Manual-de-Conduta-FIDI.pdf, respectivamente, obrigando-se, neste ato, a observá-los e cumpri-los integralmente, naquilo que lhe cabe na qualidade de contraparte da Parte Contratante, salvo se contar com programa próprio de integridade que seja considerado compatível com esse documento.

6.16. A Parte Participante deverá comunicar a FIDI sobre qualquer informação relevante que diga respeito à relação entre as Partes, no cumprimento de seu Código de Conduta ou do Código de Conduta e/ou Manual de Conduta da Parte Contratante.

6.17. No âmbito do Contrato Específico, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou ainda aceitar ou se comprometer a aceitar de quem quer que seja, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis brasileiras, por conta própria ou por terceiros, de forma direta ou indireta, devendo garantir, ainda, o cumprimento desta obrigação por seus prepostos e colaboradores.

6.18. A Parte Participante deverá manter, durante o prazo de vigência do Contrato Específico e até 5 (cinco) anos após o seu encerramento, livros, registros e contas que reflitam de maneira correta e justa, em grau de detalhamento razoável, todos os pagamentos feitos, despesas incorridas, e ativos alienados, relacionados à realização de serviços ou transações efetuadas com pagamentos e remuneração advindas do Contrato Específico, indicando a finalidade dessas ações e a pessoa (inclusive cargo e título) para quem se fez o pagamento ou despesa, sendo tais registros colocados à disposição da FIDI mediante sua solicitação.

6.19. A Parte Participante deverá guardar o sigilo das informações confidenciais obtidas durante a execução do Contrato Específico na forma das cláusulas de confidencialidade acima.

7. CONSIDERAÇÕES FINAIS

7.1. A FIDI poderá, quando o convocado não assinar o contrato no prazo estipulado, não efetuar a entrega no prazo e condições estabelecidos neste instrumento e não encaminhar a documentação exigida na cláusula 2, convocar os proponentes remanescentes na ordem de classificação, ou revogar a Coleta de Preços.

7.2. O vencedor da Coleta de Preços deverá se responsabilizar:

- Pela garantia/seguro do produto/serviço, sendo obrigatória a apresentação de documento referente a garantia (quando aplicável);

- Pela assistência técnica/suporte técnico do Produto/Serviço;

- Pela Implantação, Instalação e ou Entrega;

- Pelo treinamento da equipe na FIDI que fará uso do Produto/Serviço do mesmo;

- Pela entrega dos acessórios (quando aplicável) que acompanham o Produto descrito no Anexo I, II e III.

7.3. A FIDI emitirá pedidos de compras de fornecimento estabelecido de acordo com as suas necessidades, não se obrigando a adquirir quantidades mínimas.

8. FORO

Foro designado para julgamento de quaisquer questões judiciais resultantes desta Coleta de Preços será o da Comarca de São Paulo – SP.

São Paulo, 07 de julho de 2022.

Equipe de Suprimentos da FIDI

Anexo I

Termo de Referência

Descrição do item	Quantidade
Licenças PAM	**80 licenças**

Segue abaixo termos abaixo:

Este Termo de Referência tem por objetivo contratação de software para Gerenciamento de Acesso Privilegiado (PAM) para proteção de credenciais privilegiadas e automação do processo de acesso em formato SAAS (Software como serviço), com a prestação de serviços de implantação, treinamento, suporte técnico, manutenções corretivas e preventiva e customização.

A solução deve permitir controle granular das contas e dos ativos acessados por ela, através de um Dashboard de gestão intuitivo, controlando o ciclo de uso das credenciais.

Não deverá existir limitação para a quantidade de servidores, ativos ou credenciais de acesso configuradas na solução.

A segurança das credenciais deve estar garantida por HSM – Hardware Security Module com criptografia FIPS-140-2 nível 2. Solução certificada ISO 27001, HIPAA, SOC1 e SOC2.

REQUISITOS GERAIS DA SOLUÇÃO

Os REQUISITOS GERAIS DA SOLUÇÃO aplicam-se à Solução considerada em sua totalidade.
Os requisitos constantes deste documento têm caráter obrigatório devendo ser rigorosamente atendidos pelos fornecedores sob pena de desclassificação da proposta e sujeição à aplicação de sanções contratuais.
A solução deve ser ofertada contemplando toda infraestrutura necessária, hardware, software e serviços adicionais, necessários para o funcionamento da solução;
Todos os componentes de software da Solução deverão constar do catálogo dos respectivos fabricantes. Não serão aceitas composições ad hoc elaboradas com o objetivo de atender às especificações deste certame.

O catálogo de requisitos da solução deverá ser comprovado através de prova de conceito em caráter obrigatório ao licitante melhor classificado na fase de tomada de preços, tendo sua execução prevista para até 5 dias úteis a partir da solicitação do pregoeiro.

Todos os componentes da Solução deverão ser fornecidos com a versão mais atualizada dos softwares e firmwares considerando-se a data da implantação.

Todos os componentes de software da Solução deverão guardar total integração e compatibilidade entre si, não podendo o licitante alegar eventuais incompatibilidades de qualquer ordem para deixar de cumprir os requisitos do Edital.

A Solução deve armazenar, de forma criptografada, e controlar as credenciais de acesso privilegiado constantes dos Dispositivos Gerenciados pela Solução;

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

Eliminar credenciais privilegiadas inseridas em códigos-fonte, scripts e arquivos de configuração, fazendo com que as senhas passem a ser gerenciadas pela solução e inacessíveis às equipes de suporte e desenvolvimento de TI, terceiros e outros;

Gerar vídeos e logs de textos das sessões realizadas através da solução, armazenados em repositório seguro;

A solução em sua maioria deve ser baseada em Nuvem, a infraestrutura que hospeda a solução deve possuir elevado padrão de segurança, sendo exigido no mínimo as certificações ISO 27001, CSA STAR, SOC 1, SOC 2 e SOC 3;

A solução deverá obrigatoriamente possuir arquitetura segura de gerenciamento de privilégios segregando todos seus elementos (banco de dados e aplicações);

A parte sensível das credenciais e chaves deve ser armazenada em um hardware seguro HSM (Hardware Security Module) atestado FIPS 140 Nível 2 ou superior, o fornecedor deve dar manutenção adequada no HSM.

A solução deverá obrigatoriamente dispor de mecanismos de balanceamento de carga ou fazer uso de tecnologias de terceiros, para garantir níveis ótimos de disponibilidade e desempenho;

A solução deverá obrigatoriamente proteger a infraestrutura cloud contra ataques DDoS.

Solução de Auditoria, Gestão e Controle de Acessos Privilegiados

Conceitos gerais

A solução deve proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas;

A solução deve mitigar problemas de segurança relacionados ao compartilhamento de contas que são armazenadas localmente em dispositivos e também para as contas que não são gerenciadas centralizadamente por serviços de diretórios;
A solução deve garantir a aplicação apenas dos privilégios adequados quando provendo acesso às senhas das contas privilegiadas ao pessoal autorizado;
A solução deve proteger as senhas de credenciais compartilhadas que seriam normalmente armazenadas em planilhas e arquivos em texto claro;
A solução deve estar de acordo com a Lei Geral de Proteção de Dados (LGPD);
A solução não deverá permitir a abertura do cofre digital com chaves criptográficas geradas por seus respectivos fornecedores e/ou fabricantes;
Autenticação
A solução deve integrar-se com soluções de autenticação de duplo fator;
Deve suportar pelo menos os seguintes métodos de autenticação: Azure Active Directory, OpenID Connect e Google Authentication;
Deve suportar uso de dois fatores para autenticação através de aplicativos, e-mail e SMS;
Deve possuir mecanismo de autenticação próprio para acesso à ferramenta, com possibilidade de criação de contas e grupos sem depender de diretórios externos;
Acesso remoto
A solução deve prover facilidade de Logon Automatizado;
A solução de logon automatizado deve permitir pelo menos login em sistemas Windows baseados em Terminal Services ou Unix/Linux via SSH sem que a senha seja revelada ao operador;
A solução de acesso deve oferecer opção uso global para acessos de todos os colaboradores, de maneira que mesmo acessos não privilegiados ou com contas que não estejam armazenadas no Cofre digital (a pessoa digitará usuário e senha) possam ser realizados, agindo como servidor de ponte ou salto ou gateway de acesso;
Deverá ser possível realizar conexão transparente a ativos da rede, utilizando chaves SSH armazenadas no cofre digital como autenticação;
A monitoração e gravação das sessões privilegiadas não deve utilizar qualquer tipo de agente, ou software nos dispositivos alvo;
Deverá ser fornecido um sistema de Download e Upload seguro para transferência de arquivos durante o acesso remoto;
Deverá ser possível fazer acesso remoto a servidores Windows e Linux a partir do smartphone;
Deverá ser fornecido diferentes formas de entrada de teclado, a fim de viabilizar o uso de dispositivos móveis (smartphones) para efetuar acessos remoto;

O usuário poderá originar sessões sem passar pela interface web, iniciando seu acesso diretamente via clientes SSH ou RDP instalados em sua máquina, sem perda de funcionalidades de segurança oferecidas e sem opção de desabilitar gravação e auditoria;
Para as sessões iniciadas via cliente SSH, deverá ser dado a possibilidade de acesso através de chave público-privada, não necessitando de usuário e senha;
A função de gravação e monitoração de sessões da solução deve permitir a gravação de vídeo de sessão, e comandos digitados.
A solução deve permitir seu uso global para acessos de todos os colaboradores, de maneira que mesmo acessos não privilegiados ou com contas que não estejam armazenadas no Cofre digital (a pessoa digitará usuário e senha) possam ser realizados, agindo como um servidor de ponte ou salto ou gateway de acesso;
A solução deve ser capaz de substituir integralmente servidores de ponte ou salto ou gateway de acesso do tipo Microsoft Remote Desktop e Unix/Linux SSH, sem perda de performance ou funcionalidades especiais (Ex: clientes de acesso abertos via RemoteAPP);

Acesso remoto via terminal
A solução deve possuir modo terminal, onde o acesso possa ser solicitado diretamente ao servidor de ponte ou salto ou gateway de acesso, sem abertura da interface web de usuário, sendo que sejam suportados pelo menos o protocolo SSH para essa operação;
Deverá permitir realizar acesso utilizando chaves SSH armazenadas no cofre digital da solução como autenticação;

A solução deverá possuir mecanismo de segurança que mantenha a entrega de credenciais em caso de queda da rede ou parada total do cofre digital, evitando assim a parada de aplicações críticas;
Deverá suportar redundância de credenciais, oferecendo mais de um usuário e senha à aplicação em questão de maneira transparente, de forma que se evite qualquer possível indisponibilidade mínima durante o processo de troca de senhas;

Proxy Reverso
A solução deverá permitir o acesso em aplicações web publicadas internamente, atuando como proxy reverso com os mesmo fluxos e capacidade de compartilhamento de acessos remoto efetuados em servidores. Exemplo: Gerenciadores de código fonte, intranet;
A solução de proxy reverso deve ser viabilizada sem a necessidade de geração de novos certificados SSL, inclusões de registros de DNS e instalação de agentes na máquina do usuário ou na aplicação de destino. Este requisito visa facilitar a operação do proxy reverso;

Os acessos via proxy reverso devem obedecer aos mesmos fluxos de aprovação e autenticação estabelecidos, não sendo possível acessar os links gerados sem a devida permissão.
A solução deverá controlar e suspender os acessos através de proxy reverso sem a necessidade de intervenção na aplicação de destino;
Gestão de credenciais
A solução deve ser capaz de realizar o armazenamento e gestão de chaves SSH em sistemas Linux;
A solução deve gerenciar credenciais privilegiadas nos dispositivos de rede e segurança do ambiente;
O controle de acesso ao cofre digital é granular e permite a segregação de funções como uso da credencial, edição, visualização de logs de uso;
A solução deve ser capaz de gerenciar ilimitadas chaves SSH para ilimitados dispositivos alvo que trabalhem com as chaves;
As chaves SSH deverão ser armazenadas no cofre digital;
Deve suportar chaves nos tamanhos 1024, 2048, 4096 e 8192 bits;
Uma vez armazenadas no cofre digital, o acesso às chaves deverá ser auditado e poderá ser controlado por sistema de aprovações;
As chaves deverão poder ser gerenciadas em grupos, onde múltiplas máquinas herdam a mesma chave SSH;
Deve permitir adição de comentários à chave SSH, que deverão ser refletidos na chave SSH publica do destino, facilitando assim a administração e o rastreio do uso dessas credenciais;
A solução deve permitir que credenciais de um mesmo tipo sejam agrupadas, de modo a possuírem uma mesma senha (exemplo: todos os nós de um cluster);
Na interface web, deve haver mecanismo de busca textual para busca de credenciais, indexando qualquer campo cadastrado do objeto em questão;
A solução deve possuir esquema de aprovações para controle de revelações de senhas e conexões transparentes;
A ferramenta deve possuir relatórios de atividade, permissões de usuários e troca de senhas;
Deve permitir a integração de servidores de aplicação e o cofre digital, eliminando a necessidade de senhas e chaves SSH embutidas em aplicações, scripts e arquivos de configuração;
A solução deve armazenar as senhas e chaves única e exclusivamente no dispositivo HSM (Hardware Security Module).
Funcionalidades Visuais
A solução deverá fornecer a capacidade de customização visual e de logomarca, oferecendo templates e a possibilidade de customização completa através de CSS;
Funcionalidades Administrativas

A solução deve prover um sistema de restrição de acesso a parte Web por IP, para que apenas os IPs permitidos tenham a possibilidade de utilizar a solução;
Deve possuir mecanismo de acesso em contingência para consulta de credenciais em caso de falha da interface Web;
O cofre digital da solução deve possuir credencial de acesso emergencial (break the glass), que poderá ser utilizada obrigatoriamente através de uma chave segura impressa;
A solução deverá notificar o acesso emergencial (break the glass);
Deve possuir ferramenta própria de backup para metadados, com possibilidade de realização de atividades de backup e recuperação completas ou incrementais;
Aplicação
A solução deve fornecer uma aplicação Web para acessar as funcionalidades básicas que sejam compatíveis com o Microsoft Edge, Google Chrome e o Opera em suas últimas versões.
A solução deve ser atualizada automaticamente sem indisponibilidade do sistema, o fornecedor é o responsável pelas atualizações;
A aplicação web deve oferecer diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas aquele usuário;
A solução deve apresentar as senhas privilegiadas ao pessoal autorizado com poucos cliques após o login;
A solução deve suportar uma variedade de métodos para registrar e relatar qualquer ação realizada e detectada pela mesma, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados interna, notificações de e-mail, integração com outros frameworks e aplicações de monitoramento de terceiros;
Para melhor administração de recursos, a solução deve contar com dashboards que apresentem o status de conexão e a saúde dos componentes instalados no ambiente, permitindo visualizar no mínimo:
Quantidade de recursos, sendo estes, segredados por categoria;
Recursos com maior índice de acesso;
Últimas sessões realizadas;
Quantidade de credenciais, sendo estas, segregadas por tipo;
Listagem de credenciais mais visualizadas;
Listagem com credenciais fracas, baseado nas últimas recomendações do NIST;
Listagem com credenciais expiradas;
Deve oferecer API ou Interface REST que permita automação de operações de administração, facilitando a integração com possíveis soluções e scripts externos ao produto, com pelo menos as seguintes funções:
Gerenciamento de usuários da base interna do produto:

Adição, Remoção, Alteração e Consulta de detalhes do usuário;
Alterar Grupos do usuário.
Gerenciamento de itens do Cofre digital:
Listar, Consultar, Adicionar, Remover e Alterar itens;
Consulta, Adição, Remoção e Alteração de usuários e grupos com permissão no compartimento.
A solução deverá fornece as credenciais pelo menos via consulta de rede ou REST;
A solução deve ter mais de uma opção de idioma, sendo facultado ao usuário a opção de uso;
A solução deve oferecer ferramentas de segurança para o usuário final, tais como: gerador de senhas fortes e verificador de links seguros;
A solução deve atuar também como um Gerador de Códigos MFA, a fim de que os usuários possam pegar estes códigos dentro da mesma solução, sem ter que cadastrar outros aplicativos para este fim (ex: Google Authenticator);
Deverá integrar-se nativamente ao cofre digital da solução, utilizando sua mesma interface web;
Infraestrutura
A solução deve obrigatoriamente segregar em equipamentos diferentes as funções que armazenem dados críticos (Cofre digital e banco de dados do mesmo) de funções de front-end (interface web, servidores ponte ou de salto ou gateway de acesso, gravação, consulta de API/REST). Essa medida visa isolar componentes críticos do acesso público e geral dos usuários, permitindo a aplicação de controles de acesso e segurança de redes adequados à relevância de tais ativos;
Tanto equipamentos que armazenam dados críticos quanto de front-end devem suportar sua instalação em ambiente em nuvem, como ambientes Amazon Web Services (AWS), Microsoft Azure, Google Cloud ou outros;
Em caso de operação em ambiente em nuvem, a solução deverá possuir a devida blindagem de seus itens críticos de maneira automatizada ou fornecer procedimentos escritos de como realizá-lá;
A comunicação entre os componentes da solução deve ser autenticada e criptografada;
Nenhum dos componentes da solução deve conter senhas em texto claro para autenticação;
A solução deve permitir combinações de seus componentes instalados em equipamentos físicos, virtuais e em nuvem no mesmo ambiente, sem perda de funcionalidade;
A solução deve registrar cada acesso, incluindo os acessos via aplicação web para solicitações de senha, aprovações, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à Console de Gerenciamento tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas;
A solução deve armazenar todos os dados coletados de auditoria em um banco de dados seguro, com informações acessíveis somente via o mesmo e seus componentes;

A solução deve incorporar medidas de segurança, incluindo criptografia, a fim de proteger a informação em trânsito entre os módulos distribuídos e entre as aplicações Web dos usuários finais;
O cofre digital da solução deve utilizar HSM proprietário ou em caso de HSM de mercado, apresentar documentação comprovando a blindagem e criptografia do mesmo. A solução não deve em hipótese alguma utilizar banco de dados para armazenar credenciais como senhas privilegiadas e chaves SSH;
A base de dados da solução não deve permitir acesso externo que não seja autenticado e controlado pelo cofre digital do mesmo, evitando assim comprometimento da integridade e segurança;
A solução deve permitir sua instalação em sistemas operacionais (Windows Server ou Linux), máquinas virtuais e físicas genéricas, sem a obrigatoriedade de aquisição casada de hardware do mesmo fabricante ou appliance;
A solução deve permitir combinações de seus componentes instalados em equipamentos físicos e virtuais no mesmo ambiente, sem perda de funcionalidade;
Deve prover funcionalidade de alta disponibilidade (HA) com no mínimo dois nós, na modalidade Ativo- passivo, em que qualquer um dos nós tenha capacidade de suportar toda a carga de consultas e número total de usuários licenciados;
A solução deverá ser disponibilizada em configuração tolerante a falhas, nativa ou suportada por recursos de tolerância a falhas implementada por hardware ou software de terceiros (como o NLB ou Cluster, por exemplo).

Anexo II

Acordo de Nível de Serviço (ANS)

Grau de Severidade	Descrição	Prazo de Atendimento
1	**Inoperante** - Problema que provoca a falha total do sistema de segurança, deixando o sistema inutilizável.	8 horas úteis
2	**Grave** - Problema que provoca falha parcial do sistema de segurança ou instabilidade. Situações em que o sistema de segurança se encontra utilizáveis, entretanto, o problema inviabiliza o seu uso.	3 dias úteis
3	**Média** - Problema que provoca falha de aspectos não críticos do sistema de segurança ou apenas uma ligeira instabilidade.	7 dias úteis
4	**Porcentagem de disponibilidade dos serviços**	97%

Anexo III

Relação de Unidades de Atendimento

CNPJ FATURAMENTO	Descrição	Endereço	Nº dos CONTRATOS DE GESTÃO
CNPJ 55.401.178/0010-27	CONTRATO SEDI III	Av. Paulista, 2537 10 - º andar - Bela Vista, São Paulo - SP, 01311-300	SES - CONTRATO DE GESTAO - n.º 001.0500.000.067/2014 - SEDI 3
CNPJ 55.401.178/0005-60	CONTRATO SEDI I	Av. Paulista, 2537 10 - º andar - Bela Vista, São Paulo - SP, 01311-300	SES - CONTRATO DE GESTAO - nº 001.0500.000.009/2014 - SEDI 1