MINISTÉRIO DA SAÚDE
FUNDAÇÃO NACIONAL DE SAÚDE
COORDENAÇÃO-GERAL DE MODERNIZAÇÃO E DE TECNOLOGIA DA INFORMAÇÃO
Setor de Autarquias Sul (SAUS) – Quadra 4 – Bloco N
Brasília - CEP 70070-040
(61) 3314-6619

ANEXO I DO TERMO DE REFERÊNCIA - ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

Solução de segurança da informação para a gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC da Funasa por um período de até 36 meses, incluindo serviço de instalação e repasse de conhecimento, nos termos do presente edital e dos seus anexos.

Grupo	Item	Descrição	Unidade de medida	Quantidade	Valor Unitário	Valor Total
1	1	Solução de gerenciamento de gestão de acessos privilegiados, armazenamento de credenciais, que possibilite o isolamento, gravação e o monitoramento de sessões de ativos de TIC com serviço de garantia pelo período de 36 (sessenta) meses	Solução	1		
	2	Serviço de instalação e configuração para a solução de gestão de acessos privilegiados, armazenamento de credenciais	Serviço	1		
	3	Suporte Técnico Mensal	Serviço	36		
	4	Treinamento Técnico	Pessoa	5		

1. As licenças fornecidas para toda a solução e todos seus eventuais módulos deverão ser perpétuas, possibilitando o uso mesmo após eventual vencimento da garantia e/ou suporte. Para fins de dimensionamento do serviço técnico, considerar-se-á inicialmente os seguintes dispositivos:

Descrição	QTD
Usuários para acesso privilegiado (admin segurança/rede/Root/DomainAdmin/DBadmin/SysDBA, VMadmin, outros).	50
Estações de Trabalho de outros tipos (Tablets, Smartphones, etc.)	231
Domínios LDAP	1
Servidores físicos	79
Servidores virtuais	234 (79 Linux e 155 Windows)
Storages corporativos	25
Unidades de leitura/gravação de fitas de backup	2
Switches Core, Tor ou SAN	16
Switches de distribuição	201
Controladora WiFi	2
Appliances de segurança da informação	11
Instâncias de banco de dados	23
Instâncias servidor WEB (IIS, Apache, outros)	50
Instâncias servidor de aplicação (J2EE, .NET, Zope, etc.)	40

Instâncias servidor de correio eletrônico (MS Exchange, Postfix, Sendmail, Expresso, etc.)	4
Servidores Hipercorvergentes	8
Instâncias de servidor de gerenciamento e monitoramento de TI	1
Instâncias de servidor de gerenciamento de processos	3
Sistemas aplicativos	50
Sites WEB (Internet, intranet e extranets)	3

DA ESPECIFICAÇÃO TÉCNICA

2. ARQUITETURA DA SOLUÇÃO

2.1. O conjunto de requisitos especificados para cada item da solução pode ser atendido por meio de composição de produtos de múltiplos fabricantes/fornecedores, desde que sejam atendidas as especificações técnicas deste Termo de Referência.

2.2. A solução de gestão de acessos privilegiados deve prover auditoria e gerenciamento de acessos privilegiados por meio de credenciais privilegiadas para, pelo menos, 1.086 (mil e oitenta e seis) dispositivos (ativos de infraestrutura, servidores físicos, máquinas virtuais, sistemas tecnológicos e 15 aplicações com senha embutida (hard coded) e 50 (cinquenta) usuários simultâneos com acessos privilegiados).

2.3. A solução deverá ser entregue licenciada para ser implantada em arquitetura *on-premise* com alta disponibilidade para todas as funcionalidades, com opção ativo-ativo ou ativo-passivo local, com *failover* automático.

2.4. Deve suportar implementação no parque computacional da CONTRATANTE com, no mínimo, as seguintes especificações técnicas:

2.4.1. Windows Server 2012 e Windows Server 2016 e superior;

2.4.2. Linux (Red Hat 6, CentOS 6, Debian 8 ou Ubuntu 11 ou superiores) e Unix Solaris 11 ou AIX 7 ou superiores;

2.4.3. Ambiente de virtualização baseado em VMWare, RedHat KVM e Microsoft Hyper-V;

2.4.4. Servidores WEB e servidores de aplicação baseados nas seguintes tecnologias: Microsoft IIS, Apache e .NET;

2.4.5. Banco de Dados Microsoft SQL Server versão 2008 R2 ou superior e PostGreSQL;

2.4.6. Equipamentos de rede dos seguintes fabricantes: Cisco, Datacom, HP, Extreme e Huawei;

2.4.7. Sistemas de armazenamento de dados – Storages VNX 7500. VNX 3500 e Veritas Netbackup;

2.4.8. Ambiente de produção Microsoft Exchange Server 2012 ou superior;

2.4.9. Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo;

2.4.10. Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage);

2.4.11. Credenciais de nuvem em Azure, AWS, GCP e Office 365.

3. MODALIDADE DE FORNECIMENTO

3.1. A solução poderá ser ofertada na modalidade appliance ou virtual appliance ou instalação e configuração de máquina virtual feita pelo fornecedor.

3.2. Para as soluções ofertadas em virtual appliance ou máquina virtual, os recursos de hardware serão fornecidos pela Funasa.

3.3. A infraestrutura virtualizada a ser fornecida pela Funasa para instalação e configuração de softwares será baseada em ambiente VMWare ESXi com S.O.s Windows server e Linux.

3.4. Caso a solução seja ofertada nas modalidades previstas no item 3.2, todos os recursos computacionais, em termos de processador, memória e storage, serão provisionados tempestivamente pela Funasa durante a instalação, configuração, testes e ativação dos serviços.

4. HARDWARE DO APPLIANCE

4.1. Se ofertada na modalidade Appliance, a solução deverá contemplar o todo hardware e software necessários ao seu funcionamento e implantação no ambiente tecnológico da Funasa.

4.2. Cada servidor deverá ser instalado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

4.3. Os recursos de processamento e memória da solução Appliance deverão ser suficientes para a implementação de todas as funcionalidades descritas nesta especificação.

4.4. Todos os equipamentos necessários à prestação dos serviços devem ser novos e de primeiro uso.

4.5. Em caso de encerramento ou interrupção contratual, o hardware e todas as licenças necessárias ao funcionamento da solução serão de propriedade da Funasa.

5. ADMINISTRAÇÃO

5.1. Os servidores da solução PAM devem possuir interface WEB para uso e administração da solução.

5.2. A solução deve permitir parametrização de políticas de segurança e força de senha pelo administrador do sistema, dentre as quais:

5.2.1. quantidade mínima e máxima de caracteres,

5.2.2. conjunto mínimo de caracteres alfanuméricos e numéricos,

5.2.3. geração de senhas aleatórias e atribuição de tempo de duração de senhas.

5.3. A solução deve ser capaz de limitar a execução de comandos críticos pelos usuários cadastrados.

5.4. A solução deve permitir o controle de execução de comandos críticos por, pelo menos, “whitelist” ou “blacklist”.

5.5. A aplicação deve possuir tempo de expiração de sessão configurável pelo administrador do sistema.

5.6. A solução deve permitir o agendamento e gerenciamento de tarefas, relatórios e ações a serem realizadas automaticamente.

5.7. A solução deverá realizar sincronismo de data e relógio via protocolo NTP (Network Time Protocol) ou por meio do serviço de data e hora do sistema operacional.

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

5.9. A solução deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo SSH e HTTP/HTTPS.

6. GERENCIAMENTO DE CREDENCIAIS

6.1. 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 (quantidade de caracteres), frequência de troca da senha, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas;

6.2. Deve mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também para as contas que não são gerenciadas de forma centralizada por serviços de diretórios;

6.3. Deve descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados. Além disso, a solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas.

6.4. Deve gerenciar de forma segura as senhas utilizadas por contas de serviço com as do item acima, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos.

6.5. Deve garantir a aplicação apenas dos privilégios adequados, provendo acesso às senhas das contas privilegiadas ao pessoal autorizado.

6.6. A solução não deve limitar de maneira nenhuma o número de contas que podem ser gerenciadas em um dispositivo licenciado.

6.7. A solução, em um dispositivo licenciado, deve contemplar sua expansão, incremento ou melhoria sem qualquer custo adicional de licenciamento da solução para a CONTRATANTE.

6.8. Deve ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos.

6.9. Ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (cofre), por meio de backup ou método análogo, para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas e dados gerenciados pela solução.

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

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

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

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

6.12. Inscrever automaticamente em sistemas alvo sem aguardar por atualizações dinâmicas;

6.13. Descobrir e alterar credenciais Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, exibido em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento.

6.14. Descobrir e alterar credenciais privilegiadas em ambientes Linux e Unix.

6.15. Gerenciar credenciais em interfaces de gerenciamento de servidores "out-of-band" ou outros compatíveis com IPMI (Intelligent Platform Management Interface).

6.16. Descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP.

6.17. A solução deve possibilitar a descoberta e alteração de contas privilegiadas usadas em serviços web de forma automática ou através de adaptações via script integrados ao SDK ou API da solução. Ex: aplicações baseadas em Microsoft IIS.

6.18. Descobrir e alterar processos interdependentes e credenciais de serviço, incluindo credenciais em ambientes clusterizados.

6.19. Permitir o agrupamento lógico de sistemas a fim de simplificar a configuração de políticas apropriadas para diferentes tipos de sistemas alvo. Além de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas.

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

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

6.22. Conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH" sem que os usuários vejam qualquer senha, garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso, devendo conceder acesso a:

6.22.1. Sistemas ou aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no sistema operacional do servidor de destino, possibilitando habilitar gravação da sessão caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino.

7. GERENCIAMENTO E GRAVAÇÃO DE SESSÕES

7.1. A solução deve permitir o gerenciamento e monitoramento de sessões estabelecidas via protocolos: HTTP, HTTPS, SSH e RDP, seja via Proxy ou Jump Server.

7.2. A solução deve permitir monitoramento em tempo real das sessões ou atividades dos usuários privilegiados, disponibilizada em interface centralizada (Dashboard).

7.3. A solução deve garantir a monitoração das atividades realizadas com contas de acesso privilegiado obtidas de forma emergencial (“break-glass”).

7.4. A solução deve possuir funcionalidade de gravação das sessões dos usuários privilegiados.

7.5. A gravação de sessão de usuário deve suportar a gravação contínua de toda a sessão em vídeo e por capturas de tela.

7.6. A gravação de sessão deve possibilitar o registro da iteração do mouse e teclado durante a sessão.

7.7. A solução deve suportar a gravação da sessão de 50 (cinquenta) usuários simultâneos.

7.8. As gravações de sessão devem ser armazenadas em formato criptografado.

7.8.1. Todas as sessões acessadas devem ser gravadas possibilitando que os vídeos gerados possam ser armazenados em drivers locais de rede, pastas compartilhadas, e etc;

7.8.2. As sessões acessadas por usuários poderão ser monitoradas pelo administrador da solução, o qual, poderá bloquear e/ou interromper o acesso a qualquer tempo. Caso ocorra o bloqueio e/ou interrupção, estas ações exercidas pelo administrador também deverão ser gravadas, em formato padrão da solução, possibilitando que os vídeos gerados possam ser armazenados em drivers locais de rede, pastas compartilhadas, e etc;

7.8.3. Caso tenha formato proprietário, a solução deverá conter meios de acessar os vídeos.

7.8.4. A solução deve permitir a pesquisa textual remetendo ao momento exato em que o texto ou comando foi realizado no vídeo da gravação da sessão.

7.9. A solução deve possibilitar o gerenciamento e monitoramento de sessões das redes sociais da Funasa, acessadas via browser, como Facebook, Twitter, Instagram e Linkedin.

7.9.1. A pesquisa textual deve remeter ao momento exato em que o texto ou comando foi realizado no vídeo da gravação da sessão;

8. FLUXOS DE APROVAÇÃO

8.1. A solução deve permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características:

8.1.1. Nos fluxos de aprovação, a solução deverá permitir que seja definida uma janela temporal para as sessões. É desejável que os usuários possam apresentar uma justificativa por meio da própria solução, caso a janela temporal não atenda sua necessidade.

8.1.2. A solução deverá ser flexível no processo de aprovação para o acesso a contas privilegiadas (acessos pré-aprovados, acessos com aprovação única, acessos com aprovação dupla ou outros que possam compor a solução fornecida).

8.1.3. A solução deverá permitir a configuração de fluxos de aprovação diferenciados por criticidade e características da conta, como contas de acesso emergencial e contas de uso por terceiros.

8.1.4. Caso uma solicitação de acesso seja aprovada, a sessão e o privilégio concedido deverão expirar automaticamente ao final do período autorizado.

8.1.5. Permitir a aprovação perante um agendamento de ações administrativas, ou seja, a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos.

9. SOLUÇÃO DE SEGURANÇA PARA PRIVILÉGIOS E ACESSOS – PROTEÇÃO LOCAL PARA SERVIDORES WINDOWS

9.1. A solução de segurança de controle de elevação de privilégios deve ser entregue baseada em agentes instalados nos hosts, atender todos os 166 servidores Windows e deve permitir a remoção do privilégio administrativo dos usuários, permitindo a elevação de privilégios através de regras pré-definidas.

9.2. A solução deve possuir mecanismos para fazer a elevação de privilégios de aplicações autorizadas no Windows, a fim de atribuir o direito de administrador somente as tarefas autorizadas para cada tipo de usuário (mesmo que o mesmo não tenha direitos de administrador) e implementar a segregação de funções.

9.3. Deve garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem ser através dos monitores/gravadores de acessos), fazendo uso das funcionalidades instaladas no sistema operacional alvo.

9.4. Suportar, no mínimo, as versões Windows Server Windows Server 2008 R2, Windows, Windows Server 2012/2012 R2, Windows Server 2016 e Windows Server 2019.

9.5. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo.

9.6. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo.

9.7. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina.

9.8. A solução deve evitar que aplicativos de alto risco (como navegadores ou manipuladores de documentos) iniciem processos secundários não confiáveis, carreguem dlls não confiáveis ou explorem o PowerShell em ataques com base em conteúdo

9.9. Deve utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes.

9.10. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência.

9.11. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras.

9.12. Deve possibilitar o monitoramento e a criação de evidência em vídeo de certas execuções de arquivo e de execuções sob certas condições definidas em política.

9.13. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo.

9.14. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line.

9.15. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP.

9.16. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais.

9.17. Permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada.

9.18. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC

9.19. Suportar a guarda de políticas de hosts que não façam parte do Active Directory

9.20. Manter todas as políticas em cache e serem aplicadas ao servidor, ainda que o mesmo não esteja conectado à rede corporativa

9.21. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada

9.22. Deve possuir capacidade de emitir relatórios de aplicações e eventos de usuários inclusos na solução

9.23. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo.

9.24. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo.

9.25. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina.

9.26. Deve possibilitar o monitoramento de atividade maliciosa dos processos em execução, com a disponibilidade da opção de encaminhamento de arquivo suspeito para análise de *malware* em soluções de mercado.

10. SOLUÇÃO DE SEGURANÇA PARA PRIVILÉGIOS E ACESSOS – PROTEÇÃO PARA SERVIDORES UNIX/LINUX

10.1. A solução de segurança de controle de elevação de privilégios deve ser entregue baseada em agentes instalados nos hosts, atender todos os 65 servidores Unix e Linux deve permitir a remoção do privilégio administrativo dos usuários, permitindo a elevação de privilégios através de regras pré-definidas.

10.2. A solução deve permitir o gerenciamento dos privilégios em contas de usuário em equipamentos Unix, Linux, Solaris e AIX e associar os privilégios e comandos controlados às contas cadastradas no repositório seguro de credenciais, realizando o controle no próprio sistema operacional do destino.

10.3. A solução deverá ser capaz de garantir o controle, elevação de privilégios e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem passar pelo Cofre de senha) fazendo uso de agente instalado no sistema ou método análogo.

10.4. A solução deve implementar um modelo de delegação de privilégios mínimos, permitindo que os usuários executem qualquer comando em um nível de privilégio mais alto, desde que permitido pela política centralizada. Removendo a necessidade de os usuários efetuarem logon como root, permitindo que a conta do usuário root tenha controles de segurança muito mais restritos.

10.5. A solução deve garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino (sem passar pelos monitores/gravadores de acessos) fazendo uso das funcionalidades instaladas no sistema operacional alvo.

10.6. A solução deve disponibilizar, como conjunto mínimo de atividades controladas no ativo de destino, as seguintes operações: criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos chown e chmod e ligações entre arquivos.

10.7. Deve realizar o controle mediante interceptação do comando antes que ele seja executado.

10.8. Deve permitir a liberação de comandos privilegiados a usuários comuns.

10.9. Deve permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro de credenciais.

10.10. Deve permitir o agrupamento de comandos, bem como a utilização de coringas como (*), para uma definição ampla de parâmetros.

10.11. Deve Impedir a utilização da técnica de ShellEscape, em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos.

10.12. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução.

10.13. Monitorar e exibir acessos e atividades realizadas no próprio sistema

10.14. Prover um controle de comandos completo, com a possibilidade de criar uma lista de comandos permitidos e bloqueados (whitelisting ou blacklisting), a serem alterados (criação de alias) ou prevenir que comandos sejam executados ou permitir trabalhar em Shell modificado/controlado;

10.15. Prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas;

11. AUTENTICAÇÃO

11.1. A solução deverá ser entregue com múltiplo fator de autenticação inteligente para os acessos dos usuários, por todo período de garantia contratado, suportando:

11.2. Algorítimo de One-time Password (TOTP), compatível com pelo menos um dos seguintes aplicativos autenticadores: Google Authenticator, Authy, YubioAth, GAuth Authenticator, Authentication Codes, OATHTool, RSA SecureID, SAASPASS e 1Password;

11.3. A solução deverá possibilitar autenticação transparente no sistema-alvo, com início de sessão por meio da injeção direta de credenciais.

11.4. A solução Deve permitir aos usuários e administradores se autenticarem com duplo fator de autenticação.

11.5. A solução deverá possibilitar a utilização de área de transferência segura, de modo que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo.

11.6. A área de transferência segura deverá permitir ser desabilitada pelo administrador do sistema.

11.7. Deve prover mecanismos para mitigar ataques de força-bruta.

12. ACESSO EMERGENCIAL

12.1. Em caso de indisponibilidade, a solução deverá prover mecanismo de acesso emergencial ao cofre de senhas, como, por exemplo, o uso de contas emergenciais.

12.2. Caso haja fluxo de aprovação do acesso emergencial, a solução deve permitir a aprovação e/ou notificação dos responsáveis pela aprovação, de forma configurável.

12.3. O acionamento do acesso emergencial deve notificar os aprovadores via e-mail ou pela interface da ferramenta.

13. CRIPTOGRAFIA

13.1. A solução deverá prover mecanismos de criptografia de usuário e senha para conexão com base de dados.

13.2. 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.

13.3. A solução não deverá trafegar dados sensíveis em texto claro.

13.4. A solução deverá prover mecanismos de criptografia para informações sensíveis armazenadas em banco de dados compatível com o padrão AES com chaves de 256 bits

13.5. A interface da solução, no acesso via navegador web, deverá utilizar o protocolo HTTPS.

14. BANCO DE DADOS

14.1. O Banco de Dados deverá ser fornecido como parte integrante da solução, e deverá ser compatível com os bancos de dados já implementados na Funasa: MySQL, Oracle, SQL Server ou PostgreSQL. A proposta comercial deverá contemplar todos os custos e ações relacionados ao seu licenciamento, funcionamento, operação e segurança, exceto no caso de utilização de banco de dados SQLServer da Microsoft, para o qual a CONTRATANTE já possui licenciamento;

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

14.3. *Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues sem custos adicionais para a CONTRATANTE;*

14.4. Deve Utilizar um banco de dados que permita alta disponibilidade, e mecanismos para a recuperação de desastres e que também sejam compatíveis com soluções de backup e arquivamento disponíveis no mercado.

14.5. Caso o banco de dados utilizado seja de terceiros, a solução deverá ser entregue com licenças de software, suporte e garantia que compatibilize sua operação com a solução adquirida, sem custos adicionais para a CONTRATANTE;

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

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

14.8. Permitir a execução de Backups automatizados, permitindo a programação/agendamento de horários;

15. COMPATIBILIDADE

15.1. A solução deverá ser integrada à base de usuários com privilégios administrativos do Microsoft Active Directory e RADIUS (Remote Authentication Dial-in User Service) da rede da Funasa para concessão de perfis de acesso às ferramentas implementadas.

15.2. Os componentes da solução proposta deverão ser capazes de operar por interface gráfica acessada por navegador web compatível com os padrões W3C.

15.3. A solução deverá permitir o gerenciamento e monitoramento de sessões do Microsoft Azure, AWS e Google Cloud.

15.4. A solução deverá ser compatível com pelo menos dois dos seguintes navegadores: Google Chrome, Firefox e MS Edge.

15.5. A solução deverá ser compatível com a tecnologia VMware/VSphere v6.5 ou superior.

15.6. A solução deve suportar acesso via dispositivos móveis como tablets e smartphones.

15.7. A solução deverá permitir o gerenciamento e monitoramento de sessões nos Sistemas Gerenciadores de Bancos de Dados: Oracle, MS SQL Server e MySQL.

15.8. A solução deverá possibilitar a replicação em outros Data Centers.

16. USUÁRIOS E GRUPOS

16.1. A solução deve permitir a criação de grupos de usuários.

16.2. A solução deve permitir a atribuição de privilégios a grupos de usuários, associados a um ou mais alvos gerenciados.

16.3. A solução deve permitir acesso simultâneo ao cofre de senhas e às contas privilegiadas por dois ou mais usuários.

16.4. A solução deve viabilizar a segregação de funções entre usuários de uma mesma aplicação gerenciada.

16.5. A solução deve prover funcionalidade para revogar todos os acessos de um usuário cadastrado de maneira imediata.

17. CONTAS DE SERVIÇO

17.1. A solução deve ser capaz de gerenciar senhas privilegiadas de aplicações, de modo a evitar senhas embutidas em códigos-fonte.

17.2. A solução deverá disponibilizar a troca de senhas dos sistemas gerenciados, de forma individual ou por grupos customizáveis (grupo de todos os sistemas operacionais UNIX, por exemplo).

17.3. A troca periódica das senhas de aplicações deve ser feita de forma transparente, sem a necessidade de desligamento ou reinicialização de sistemas.

18. NOTIFICAÇÕES E ALERTAS

18.1. A solução deverá enviar notificação por e-mail ao aprovador a cada nova solicitação de acesso.

18.2. As notificações ou alertas emitidos pela solução devem ser customizáveis.

18.3. A solução deverá manter a persistência de todos os relatórios e arquivos históricos, incluindo gravações de sessão, sem necessidade de restauração de backup, por pelo menos 90 (noventa) dias.

18.4. A solução deverá permitir **retenção em backup** de relatórios e logs da aplicação por, pelo menos, 2 (dois) anos.

18.5. A solução deve permitir **retenção em backup** das gravações de sessão por, pelo menos, 1 (um) ano.

18.6. A solução deverá permitir a integração com ferramentas de *backup* de mercado.

19. ATUALIZAÇÃO DE VERSÕES

19.1. Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada, e prover mecanismos de atualização de segurança de forma automática e sob demanda por meio de interface gráfica intuitiva.

19.2. Os equipamentos e softwares não podem constar, no momento da apresentação da proposta técnica, em listas de *end-of-sale, end-of-support, end-of-life* ou similares do fabricante em prazo superior ao da vigência contratual, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida.

19.3. O fornecedor deverá manter, nas novas versões e atualizações de serviços e funções, a compatibilidade com o sistema inicialmente entregue.

20. RELATÓRIOS

20.1. Os módulos de visualização de sessões e geração de relatórios devem exibir filtros de pesquisa para logs e sessões gravadas, com pelo menos os seguintes campos: palavra-chave, usuário responsável pela ação, aprovador, dispositivo ou sistema alvo acessado e período de consulta.

20.2. A solução deve permitir a exportação de relatórios no mínimo à dois formatos: HTML, PDF, XML ou CSV.

20.3. A solução deve permitir a geração de relatório de todos os usuários cadastrados na aplicação, e seus respectivos papéis.

20.4. A solução deve permitir a geração de relatório de contas de usuários privilegiados monitoradas pela ferramenta.

20.5. A solução deve possuir mecanismos para geração de relatórios a respeito das contas privilegiadas, tais como listas de ativos e suas contas gerenciadas, requisições de acesso a contas privilegiadas submetidas à aprovação, aprovadas ou rejeitadas e histórico de utilização das contas privilegiadas.

21. LOGS E AUDITORIA

21.1. A solução deve possuir trilha de auditoria sobre a aplicação de regras para cada conta de acesso privilegiado.

21.2. A solução deve possibilitar o rastreamento de todas as ações realizadas nos sistemas gerenciados por meio das contas privilegiadas.

21.3. A solução deverá permitir integração com ferramentas de SIEM de acordo com os padrões de mercado, por meio de provisionamento de informações ou envio automático de logs para servidores SYSLOG, aderente aos princípios da RFC 5424.

22. INTERFACE

22.1. O sistema deve disponibilizar a exibição de menus e telas configuráveis para os idiomas português e inglês.

22.2. A aplicação deve permitir personalização de estilo, como alterações de cores e/ou inclusão de logo/banner, para receber a identidade visual da Funasa.

23. COMPROVAÇÃO DE REQUISITOS

23.1. Para fins de aceitação, pela Funasa, todas as especificações técnicas descritas deverão ser comprovadas ponto a ponto através de catálogos, folders, e manuais da solução indicando corretamente a página, o documento e o trecho de comprovação em arquivo digital editável, por exemplo: *word ou excel*, que demonstre o atendimento de cada item/subitem da especificação técnica.

23.2. A Funasa se reservará ao direito de aferir, em prova de conceito da solução em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei.

24. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

24.1. Os serviços de implantação da Solução são compostos de instalação, ativação, customização, integração, documentação, suporte técnico e logístico e gerência da implantação dos diversos componentes da Solução, além de definição do processo de administração, gestão das credenciais privilegiadas, treinamento e transferência de conhecimento técnico sobre os componentes da Solução.

24.2. As atividades de instalação, ativação, customização e integração compreendem todos os procedimentos relacionados à instalação, ativação e configuração da Solução, incluindo parametrização e testes de quaisquer componentes de software fornecidos no escopo do
Edital, de modo a garantir o pleno funcionamento da Solução, inclusive garantindo a operacionalização e integração com os demais componentes de hardware e software atualmente em uso na rede do CONTRATANTE.

24.3. Todos os componentes de software requeridos para atender as funcionalidades exigidas no Edital, mesmo que não estejam especificados e cotados na proposta, serão considerados como parte integrante dos serviços de instalação e deverão ser fornecidos, sem ônus adicional para o CONTRATANTE.

24.4. As atividades de definição do processo de administração das credenciais privilegiadas compreendem:

24.4.1. especificar, documentar, validar, parametrizar, configurar e customizar as políticas com a definição de quais as premissas, características e restrições de cada tipo de permissão;

24.4.2. especificar, documentar, validar, parametrizar, configurar e customizar, quando for o caso, os fluxos de aprovações;

24.4.3. realizar a capacitação com a equipe da CONTRATANTE para parametrizar, configurar e customizar as políticas e fluxos das credenciais privilegiadas na solução.

24.4.4. As atividades de gestão das credenciais privilegiadas compreendem a administração completa da credencial, assim como o armazenamento e a troca automática da senha da credencial privilegiada em todos os locais utilizados da credencial.

24.4.5. Todos os documentos da Solução devem ter o ACEITE pelo CONTRATANTE.

24.5. O serviço de instalação da Solução deverá descrever os procedimentos e prazos necessários para a execução das atividades de implantação. Deverá ser composto, no mínimo, pelos seguintes documentos:

24.5.1. Desenho da Arquitetura da Solução, contemplando:

24.5.1.1. proposição de desenho da Solução, detalhando os cenários e topologias propostos;

24.5.1.2. topologia dos clusters de máquinas hospedeiras (hosts);

24.5.1.3. topologia das interconexões lógicas LAN (Local Area Network) e SAN (Storage AreaNetwork).

24.5.1.4. considerar a instalação em alta disponibilidade, com cluster ativo – ativo, no sítio primário e no sítio secundário com redundância da base de dados entre os sítios.

24.5.1.5. deverá contemplar as atividades de monitoramento, backup e restore.

24.6. O CONTRATADO deverá elaborar o Guia de Processo de Administração das Credenciais, contemplando:

24.7. guia de políticas por tipo de credenciais;

24.8. guia de fluxos de aprovações;

24.9. guia de acesso emergencial (break glass);

24.10. guia de Backup e Restore;

24.11. guia de desligamento e religamento da solução.

24.12. Caso haja inconsistência entre componentes previstos na proposta técnica da Solução apresentada pelo CONTRATADO e os de fato entregues ao CONTRATANTE, este notificará o CONTRATADO formalmente a respeito da inconsistência, ficando reservado ao CONTRATANTE o direito de recusar-se a receber tais componentes, além da aplicação de eventuais sanções previstas no instrumento contratual.

24.12.1. Todo componente entregue em desacordo com os requisitos do Edital ou com a proposta técnica fornecida pelo CONTRATADO, deverá ser substituído, bem como deverão ser supridos aqueles componentes cuja falta seja verificada em relação à citada proposta técnica, obedecido, em ambos os casos, os prazos de entrega definidos neste Edital.

24.12.2. Serão de inteira responsabilidade e a expensas do CONTRATADO, sem nenhum custo adicional para o CONTRATANTE:

I - Atividades de prospecção, concepção, projeto, planejamento, implementação, suporte técnico, assistência técnica e apoio logísticos necessários à adequada implantação da
Solução;

II - Implantação da Solução, incluindo o apoio e suporte técnico e logísticos eventualmente necessários ao adequado funcionamento da Solução;

III - Alocação de profissionais qualificados e todas as obrigações trabalhistas relacionadas;

IV - Configuração lógica dos componentes da Solução proposta de forma a viabilizar integralmente os testes a serem realizados como parte da homologação da Solução e o adequado funcionamento em ambiente de produção;

V - Demonstração de todas as características técnicas e funcionalidades previstas na contratação, durante a fase de implantação da Solução;

VI - Identificação do quadro de profissionais alocados na disponibilização da Solução;

VII - Todos os ônus relativos a transporte, alimentação e hospedagem de profissionais, transporte e instalação dos equipamentos, ligações telefônicas para suporte técnico, disponibilização de ferramentas (físicas e lógicas) além de insumos diversos requeridos durante quaisquer das fases de homologação e implantação da Solução;

24.13. Após a conclusão de implantação da solução o CONTRATADO deverá acompanhar presencialmente a operação junto com a CONTRATANTE durante 10 dias úteis para:

24.13.1. auxílio na elaboração de procedimentos:

24.13.2. operacionais: como executar backups, como monitorar espaço em disco, uso de CPU, tratamento de alertas etc;

24.13.3. de Criação de perfis para Usuários, aprovadores e administradores, com configurar restrições de horários, fluxo de aprovação etc;

24.13.4. para inclusão de novos dispositivos dentro do cofre de senha, como configurar acessos, alertas, executar varreduras para manter a conformidade do ambiente;

24.13.5. criação, agendamento e geração de relatórios. Como enviar para os responsáveis pelos dispositivos etc;

24.13.6. consultoria e auxílio no processo de movimentação dos demais dispositivos para dentro do cofre não foram inclusos no serviço de implantação;

25. SUPORTE TÉCNICO MENSAL

25.1. A contratada deverá fornecer o suporte da solução período mínimo de 36 (trinta e seis) meses contados da emissão do Termo de Recebimento Definitivo para garantia de atualizações de versão, suporte técnico e acionamento em nível de resolução de problemas pelo próprio fabricante, e apoiar a Funasa na resolução de demandas junto ao fabricante;

25.2. O serviço de suporte técnico compreende:

25.2.1. O atendimento para identificação e correção de falhas ou inconsistências detectadas nos produtos da solução, inclusive nas suas configurações e parametrizações, também se aplica na prestação de informações necessárias ao esclarecimento de dúvidas, de forma a garantir o perfeito funcionamento e utilização dos softwares e hardwares, de acordo com o estabelecido nos manuais que acompanham o produto.

25.2.2. Adaptações que possam decorrer de necessidade da Funasa, ao longo da vigência contratual, por exemplo;

25.2.2.1. Realizar adaptações que demandem desenvolvimento de scripts, automações, dashboards e congêneres;

25.2.2.2. Integração da solução com novas tecnologias adquiridas pela Funasa, em razão da expansão ou melhorias técnicas no ambiente, que podem compreender;

25.2.2.2.1 Ativos de rede e segurança (switches, roteadores, firewalls, Controladores, WiFi, etc;

25.2.2.2.2 Domain Controllers;

25.2.2.2.3 Instâncias de Banco de Dados;

25.2.2.2.4 Configuração da solução para permitir integração com sistemas e/ou aplicações, que sejam fornecidos com sua Interface de Programação de Aplicação (em inglês, Applica□on Programming Interface - API) ou SDK (Soware Development Kit), nos formatos XML ou JSON;

25.2.2.2.5 Nova instalação da solução em caso de recuperação de desastre de ambiente, com configuração mínima compatível com o ambiente original.

25.3. A CONTRATADA deverá fornecer correções de bugs ou alternativa para corrigir defeitos nos softwares indicados neste Termo de Referência, que façam com que eles não operem de acordo com a documentação publicada para os usuários dos softwares.

25.4. O suporte técnico e o atendimento deverão ser prestado em escala 24 (vinte e quatro) horas por dia, 7 (sete) dias da semana , durante o período de vigência do contrato, em português brasileiro.

25.5. Para operacionalização do suporte técnico, a CONTRATADA deverá disponibilizar uma área em sítio da Web voltada para a abertura dos chamados técnicos.

25.6. Como forma de atendimento paliativo a comunicação poderá ser através de uma central de atendimento telefônica e/ou endereços de correio eletrônico (e-mail);

25.7. Toda e qualquer solicitação feita pela CONTRATANTE deverá ser registrada pela CONTRATADA, em sistema informatizado para acompanhamento e controle da execução dos serviços.

25.8. Caso a solução do problema do chamado técnico exija a presença de analista da CONTRATADA nas dependências do CONTRATANTE, mesmo fora do horário comercial, este deverá ficar dedicado a resolução do problema até que ele esteja resolvido.

25.9. A CONTRATADA será responsável pelo fornecimento de informações sobre novas versões dos sistemas, bem como sua respectiva documentação técnica.

25.10. Identificação, diagnóstico e aplicação de correções de problemas no ambiente operacional do software.

25.11. Atendimento a solicitações de suporte técnico relacionadas às adaptações, ajustes, problemas, erros apresentados, dúvidas e forma correta de utilização da solução CONTRATADA, fornecendo as informações, orientações técnicas ou correções e/ou adaptações e ajustes necessários ao restabelecimento da normalidade.

25.12. O suporte técnico deverá ser prestado para a solução e deverá ser acionado em caso de qualquer indisponibilidade da solução, devendo haver o atendimento on-site, se requerido pelo contratante, conforme os índices de criticidade a seguir:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto na operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial	Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas

	dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 15 min. um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Entrega da Solução pelo fabricante em até 6 dias.
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas
			Entrega da Solução pelo fabricante em até 10 dias.

Severidade 3	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.
		No mesmo dia ou no próximo dia útil comercial	No mesmo dia ou no próximo dia útil comercial

25.13. Cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante,

25.14. Deverá ser fornecido um serviço a nível mundial de monitoramento proativo para ameaças de segurança que encaminhe notificações técnicas via e-mail.

25.15. Deve possibilitar a abertura de chamados de suporte, para no mínimo, os métodos: telefone 0800, e-mail, site do fabricante.

25.16. A cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante;

25.17. Deve possibilitar a abertura de chamados de suporte, para no mínimo, os métodos: telefone 0800, e-mail, site do fabricante;

25.18. Todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura o chamado independentemente deste ter sido feito via telefone, email, site da contratada ou do fabricante;

25.19. O período de suporte deve estar diretamente atrelado ao período de garantia da solução;

25.20. Dentro do prazo máximo de solução está compreendido o prazo de atendimento;

25.21. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado;

25.22. Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;

25.23. Os serviços de atendimento de garantia para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados);

25.24. Os chamados de garantia de severidades 1 e 2 deverão contar com suporte in loco da contratada para prover celeridade no restabelecimento do serviço;

25.25. O fornecedor emitirá relatório sempre que solicitado pelo contratante, em arquivo eletrônico, preferencialmente em arquivo texto, com informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período, incluindo:

1. Quantidade de ocorrências (chamados) registradas no período;
2. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura; Data e hora de abertura;
3. Data e hora de inicio e conclusão do atendimento;
4. Identificação do técnico do contratante que registrou o chamado;
5. Identificação do técnico do contratante que atendeu o chamado da garantia; Descrição do problema;
6. Descrição da solução;
7. Informações sobre eventuais escalações;
8. Resumo com a lista de chamados concluídos fora do prazo de solução estabelecido;
9. Total de chamados no mês e o total acumulado até a apresentação do relatório;

25.26. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

26. TREINAMENTO TÉCNICO

26.1. A CONTRATADA deverá ministrar um workshop de treinamento presencial da solução que será de, no mínimo, 20 horas, com emissão de certificado oficial aos participantes.

26.2. O treinamento será realizado no modelo presencial, em português, utilizando ferramenta própria disponibilizada pela fabricante.

26.3. A CONTRATADA disponibilizará espaço físico, estrutura lógica, internet, computadores e materiais de estudo em português e/ou inglês, ou seja, todos os insumos necessários para a serem utilizados pelos participantes do curso.

26.4. O treinamento deverá possuir carga horária total de, no mínimo, 20h (vinte horas) e o seu conteúdo deverá estar em consonância com os modelos e versões dos produtos da Solução contratada e abranger os aspectos de instalação, configuração, gerenciamento, administração e troubleshooting da Solução.

26.5. O treinamento deverá ser ministrado em dias úteis, no horário comercial, não devendo exceder o limite de 4h (quatro horas) diárias.

26.6. Deverá ser realizado por profissional certificado pelo fabricante, tendo a qualificação técnica necessária quanto à instalação, configuração e gerenciamento da solução adquirida.

26.7. O recebimento definitivo e atesto para pagamento do treinamento só será feito, após o recebimento do certificado de conclusão emitido pela CONTRATADA.

Documento assinado eletronicamente por **Andre Wilson Pimenta Santana**, **Coordenador(a)**, em 09/08/2021, às 10:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Telvio Martins de Mello**, **Coordenador-Geral de Modernização e de Tecnologia da Informação**, em 09/08/2021, às 14:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marcio Biage da Silveira**, **Chefe do Serviço de Compras e Contratos**, em 09/08/2021, às 15:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.funasa.gov.br/consulta, informando o código verificador **3103691** e o código CRC **1A9F9816**.

Referência: Processo nº 25100.000334/2020-38 SEI nº 3103691