

ESPECIFICAÇÃO TÉCNICA SOLUÇÃO PAM (PRIVILEGED ACCESS MANAGEMENT)

1. DESCRIÇÃO GERAL DA SOLUÇÃO

1.1. Requisitos gerais dos serviços

- 1.1.1. A solução deverá possuir painel destinado ao gerenciamento e controle de permissões e privilégios em infraestruturas de nuvem, garantindo segurança e conformidade em ambientes multi-cloud e híbridos.
- 1.1.2. Deverá prover administração consolidada de acessos, assegurando visibilidade avançada, controle rígido de privilégios e resposta proativa a ameaças, contemplando no mínimo:
 - 1.1.2.1. Inventário com monitoramento e auditoria de todas as permissões e acessos concedidos em provedores de nuvem como AWS, Azure e GCP;
 - 1.1.2.2. Mapeamento detalhado de privilégios por usuário, serviço ou grupo, permitindo identificar excessos de permissões;
 - 1.1.2.3. Utilização de mecanismos de análise comportamental, incluindo Machine Learning e/ou Inteligência Artificial, para detecção de anomalias em acessos e atividades;
 - 1.1.2.4. Recomendações automáticas para ajuste de políticas de acesso, com base no princípio do menor privilégio;
 - 1.1.2.5. Trilha de auditoria com registro completo e imutável de ações e alterações de permissões;
 - 1.1.2.6. Monitoramento em tempo real das atividades de acesso e alterações;
 - 1.1.2.7. Geração de alertas e notificações imediatas para comportamentos suspeitos ou não conformidades.
- 1.1.3. A solução deverá permitir a automatização de políticas de segurança baseadas no modelo Zero Trust, com detecção e correção automática de permissões excessivas ou inadequadas, conforme políticas predefinidas.
- 1.1.4. Gerenciamento de credenciais privilegiadas:
 - 1.1.4.1. A solução deverá realizar: descoberta de contas privilegiadas; rotação das senhas; aprovação para acesso a servidores, ativos de redes, bancos de dados e aplicações desconectadas; gravação das sessões; auditoria de comandos e das sessões; auditoria de uso das credenciais; bloqueios a partir de blacklists de comandos; monitoramento das sessões em tempo real.
- 1.1.5. Gerenciamento das sessões:
 - 1.1.5.1. A solução deverá permitir: o acesso aos dispositivos alvo deverá ser realizado sem a necessidade digitar as credenciais; registro em vídeo da sessão; implantação de workflows de aprovação para liberar as sessões; controle de horários de acessos e endereços de IP aprovados; liberar acesso somente a determinadas aplicações ao invés de todo o sistema operacional; acompanhamento em tempo real e simultâneo de uma conexão remota.
- 1.1.6. Automatização de comandos:
 - 1.1.6.1. A solução deverá permitir a automação de comandos privilegiados, podendo ser por meio de scripts ou tarefas previamente configuradas na solução de PAM, sem que haja necessidade de acesso ao dispositivo alvo (servidor, por exemplo).
- 1.1.7. Alta disponibilidade:
 - 1.1.7.1. A solução deverá atuar em Alta Disponibilidade no ambiente de produção da CONTRATADA. Garantindo que em caso de desastre (perda total do acesso da solução de PAM) seja possível recuperar as credenciais privilegiadas de forma rápida e eficiente. De modo que os acessos aos dispositivos alvo possam ocorrer sem a necessidade de se recuperar o ambiente da solução de PAM.
- 1.1.8. Análise comportamental e ações automatizadas com identificação de movimentação lateral:

- 1.1.8.1. A ferramenta deverá: estudar e traçar as rotinas dos usuários, e caso identificar algo incomum, permitir gerar ações automáticas ou manuais de bloqueios;
- 1.1.8.2. Identificar a criação de credenciais privilegiadas nos dispositivos alvos (que visam posterior acesso por fora da solução de PAM, caracterizando a movimentação lateral) e armazená-las de forma automática através de mecanismos de Scan e Discovery, por exemplo.
- 1.1.8.3. Realizar a rotação das credenciais ora armazenadas, visando impedir acessos por fora da ferramenta.
- 1.1.9. Controle de acessos temporários a Bancos de Dados:
 - 1.1.9.1. A solução deverá permitir conceder acessos temporários (com prazo para encerramento da sessão) em bancos de dados, com monitoramento, auditoria e controle da sessão. Garantindo que ao terminar a execução das tarefas no Banco de Dados, a sessão seja encerrada e o acesso finalizado, necessitando de novo acesso posteriormente.
- 1.1.10. Armazenamento dos relatórios de auditoria e gravação das sessões:
 - 1.1.10.1. A periodicidade de retenção de logs e gravação das sessões deverá ser personalizada.
 - 1.1.10.2. Deverá ter a possibilidade de armazenar os logs de acordo com o tempo do serviço SaaS contratado.
 - 1.1.10.3. A solução deverá possuir mecanismo nativo de compressão das gravações das sessões, visando otimizar o consumo de armazenamento.
- 1.1.11. Gestão de níveis de perfis:
 - 1.1.11.1. A solução deverá garantir que haja o controle de níveis de perfis de acesso dos usuários de acordo com a necessidade da CONTRATADA.
- 1.1.12. Importação dos dispositivos alvos/Discovery:
 - 1.1.12.1. A solução deverá permitir importar os dispositivos alvo (servidores, bancos de dados, ativos etc.), através de Scan e Discovery automatizado e por alguma das seguintes extensões de arquivos: CSV, XLS, XLSX.
- 1.1.13. Provisionamento de recursos:
 - 1.1.13.1. A Solução deverá estar acompanhada de todo o licenciamento necessário para seu pleno funcionamento, a ser fornecido pela CONTRATADA;
 - 1.1.13.2. O licenciamento da solução deverá abranger o suporte técnico do fabricante de componentes adicionais, como por exemplo, mas não se limitando, a Banco de Dados e Sistema Operacional.
- 1.1.14. Armazenamento de credenciais de “sistemas desconectados”:
 - 1.1.14.1. Considera-se uma “credencial de sistema desconectado”, aquela utilizada para acesso a planilhas, aplicação e sistemas que não são integrados ao PAM.
 - 1.1.14.2. A solução deverá permitir o armazenamento das credenciais citadas no item imediatamente anterior a este de forma manual, onde o administrador da ferramenta realizará o cadastro.
- 1.1.15. A Solução deve ser disponibilizada na modalidade em Nuvem (Cloud) do FABRICANTE, disponibilizando o direito ao CONTRATANTE o uso da Solução pelo período de vigência do contrato.
- 1.1.16. A Solução deve ter seu horário ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).
- 1.1.17. A Solução deve possuir todas as interfaces com o usuário do sistema e mensagens, preferencialmente, em português (Brasil). Não sendo possível, deverá apresentá-las, obrigatoriamente, em inglês.

- 1.1.18. A solução ofertada deve ser instalada em sua última versão estável e estar coberta por contrato de suporte e atualização de versão do fabricante durante a vigência da garantia.
- 1.1.19. Os produtos que compõem a solução não devem estar com término de comercialização (End-of-Sale) anunciado, isto é, os produtos devem estar em produção e serem comercializados pelo fabricante no momento da assinatura do Pedido de Compra/Contrato. Após ser anunciado o término da comercialização (End-of-Sale) dos produtos que compõem a solução, o suporte (End-of-Support) deverá permanecer por, no mínimo, o período de vigência da garantia.
- 1.1.20. Deve possuir interface de gerenciamento web para acesso às funcionalidades da solução e suportar, no mínimo, as versões de navegadores Microsoft Edge, Google Chrome e Mozilla Firefox.
- 1.1.21. Não deve exigir a instalação de software adicional em equipamentos da CONTRATANTE, exceto agentes para gestão de elevação de privilégios.
- 1.1.22. Não será permitida a composição de softwares de terceiros para o atendimento aos requisitos técnicos, exceto se nativamente suportado pela solução e com o respectivo suporte técnico do fornecedor/fabricante.
- 1.1.23. Deve possuir interface única, na mesma solução, para o gerenciamento de contas, senhas, sessões e ativos agregados ao cofre de senhas.
- 1.1.24. Deve suportar para os processos de autenticação e autorização, o padrão MFA.
- 1.1.25. A senha dos usuários colaboradores da CONTRATANTE não deverá ser armazenada ou conhecida pela Solução.
- 1.1.26. Deve permitir bloquear as tentativas de liberação, atualização e remoção de acessos diretamente da solução CONTRATADA, quando integrado com a solução de Governança e Administração de Identidades (Serviço de Diretório LDAP) da CONTRATANTE.
- 1.1.27. Deve garantir que não será permitida à CONTRATADA qualquer modalidade de tratamento sobre os dados pessoais fornecidos pela CONTRATANTE, para finalidades além daquelas previstas no projeto ou sem a expressa autorização da CONTRATANTE por meio de comunicação oficial.
- 1.1.28. Deve, em caso de eventual tratamento de dados pessoais por parte da CONTRATADA, responsabilizar-se pelos dados pessoais de usuários da CONTRATANTE no papel de operador desses dados, sob pena de responsabilidade conforme prevista na legislação brasileira.
- 1.1.29. Deve comunicar à CONTRATANTE, de forma imediata, qualquer evento decorrente de tratamento de dados pessoais de usuários por parte da CONTRATADA, que possa ser considerada violação de dados pessoais no entendimento da Lei 13.709/2018, assim como qualquer fato que possa acarretar dúvida na interpretação desta lei com relação ao tratamento de dados pessoais deverá ser discutida com a CONTRATANTE.
- 1.1.30. Deve garantir que os dados da CONTRATANTE não serão enviados a terceiros, sem conhecimento e autorização prévia da CONTRATANTE.
- 1.1.31. Deve garantir que as exigências elencadas neste documento não eximem a responsabilidade da CONTRATADA quanto ao cumprimento de outros dispositivos presentes na legislação pertinente à proteção de dados pessoais vigentes no Brasil.

1.2. Do Modelo de Entrega – Solução Como Serviço (saas)

- 1.2.1. A solução de Gerenciamento de Acessos Privilegiados (PAM) deverá ser fornecida integralmente no modelo SaaS (Software as a Service), ou seja, executado em ambiente de nuvem da

CONTRATADA ou nuvem pública, sem necessidade de instalação local de servidores, banco de dados ou infraestrutura na rede do SENAC ES.

1.2.2. A arquitetura da solução deverá seguir o modelo nativo em nuvem, disponibilizada por meio de internet, com acesso por navegadores web atualizados, utilizando conexões seguras (HTTPS/TLS 1.2 ou superior).

1.2.3. A CONTRATADA será inteiramente responsável pela infraestrutura necessária para operação da solução, incluindo:

- Atualizações automáticas e contínuas da plataforma;
- Gerenciamento de patches, correções de vulnerabilidades e novas funcionalidades;
- Garantia de alta disponibilidade da solução, conforme SLA mínimo de 99,5% mensal;
- Monitoramento proativo e proteção contra falhas, com plano de recuperação de desastres.

1.2.4. A solução SaaS deverá oferecer os seguintes recursos:

- Escalabilidade automática, conforme aumento no número de usuários, ativos gerenciados ou volume de sessões simultâneas;
- Isolamento lógico entre ambientes de clientes distintos (multitenancy seguro);
- Ambiente redundante geograficamente para continuidade de negócios;
- Acesso controlado e seguro, com autenticação multifator e restrição por IP, horário e localização geográfica;
- Interface administrativa e de auditoria 100% web, sem dependência de plugins ou instalação de agentes obrigatórios no dispositivo de gestão.

1.2.5. A CONTRATA deverá disponibilizar ao SENAC ES:

- Painel de administração para configuração e gerenciamento completo da solução;
- Painel de relatórios, logs e auditorias;
- Portal de suporte técnico com base de conhecimento, abertura de chamados e acompanhamentos;
- SLA detalhado com prazos de resposta e solução para incidentes e requisições.

1.2.6. Os dados do SENAC ES devem permanecer sob propriedade exclusiva da CONTRATANTE, sendo vedada sua utilização pela CONTRATADA para quaisquer outras finalidades além da prestação dos serviços.

1.2.7. A CONTRATADA deverá garantir:

- Portabilidade dos dados ao final do contrato, em formato aberto ou estruturado;
- Possibilidade de exportação dos dados e logs a qualquer momento mediante solicitação;
- Processo claro de exclusão segura dos dados, com fornecimento de termo de eliminação, quando solicitado.

1.3. Integração com Ferramentas

1.3.1. A solução de Privileged Access Management (PAM) deverá oferecer suporte nativo ou via APIs RESTful para integração com ferramentas de ITSM (Information Technology Service Management), SIEM (Security Information and Event Management), com o objetivo de garantir automação, visibilidade e capacidade de resposta ampliada em todo o ecossistema de segurança e governança da organização.

1.3.2. Integração com ITSM

1.3.2.1. A solução deverá permitir vincular requisições de acesso privilegiado a tickets de chamados previamente abertos e aprovados em sistemas ITSM.

1.3.2.2. Funcionalidades mínimas exigidas:

Serviço Nacional de Aprendizagem Comercial
Departamento Regional no Espírito Santo

- 1.3.2.2.1. Validação automática de número de ticket válido antes da liberação de credenciais.
- 1.3.2.2.2. Integração com workflows de aprovação para acessos JIT (Just-in-Time).
- 1.3.2.2.3. Registro automático da sessão iniciada via PAM no chamado correspondente.
- 1.3.2.2.4. Capacidade de iniciar sessão privilegiada diretamente a partir do chamado aprovado.
- 1.3.2.2.5. Compatibilidade com ferramentas que utilizem API REST, SOAP ou conectores nativos.

1.3.3. Integração com SIEM

- 1.3.3.1. A solução deverá ser capaz de exportar eventos, alertas e logs de auditoria para ferramenta de SIEM em tempo real.
- 1.3.3.2. Funcionalidades mínimas exigidas:
 - 1.3.3.2.1. Envio de logs estruturados em formatos padrão (CEF, JSON, Syslog, LEEF etc.).
 - 1.3.3.2.2. Geração de eventos, alertas de risco, tentativas de acesso negado, uso de break-glass, entre outros.
 - 1.3.3.2.3. Capacidade de associar eventos de sessão com identidade, localidade, IP de origem, dispositivo acessado e motivo do acesso.
 - 1.3.3.2.4. Mecanismos de autenticação segura para integração com o SIEM (ex.: TLS, API keys).
 - 1.3.3.2.5. Geração de dashboards de segurança e trilhas de auditoria customizadas para análise forense e conformidade.

1.3.4. Requisitos adicionais de Integração

- 1.3.4.1. A solução deverá dispor de documentação oficial e pública para as integrações, incluindo exemplos de configuração e suporte técnico.
- 1.3.4.2. As integrações deverão seguir os princípios de segurança da informação, com controle de acesso baseado em perfis e uso de autenticação segura (ex.: OAuth2, certificados, API Keys com escopo limitado).
- 1.3.4.3. A solução deverá possuir mecanismos para controle de falhas de integração e geração de alertas em caso de interrupções ou falhas críticas nos conectores.
- 1.3.4.4. Todas as integrações devem ser compatíveis com ambientes híbridos (on-premise e cloud) e multiplataforma.

2. COFRE DE SENHAS

2.1. Do Armazenamento Seguro e Controle de Credenciais Privilegiadas

- 2.1.1. A solução deve contemplar um módulo de Cofre de Senhas (Password Vault) destinado ao armazenamento seguro, gerenciamento e rotação automática de credenciais privilegiadas. O cofre deve oferecer:
 - 2.1.1.1. Armazenamento criptografado de senhas em conformidade com padrões como FIPS 140-2.
 - 2.1.1.2. Suporte à rotação automática de senhas com agendamento por grupo, usuário ou tipo de sistema.
 - 2.1.1.3. Intermediação de acesso sem exposição das credenciais ao usuário final.
 - 2.1.1.4. Controle baseado em políticas, com aprovação por workflow e tempo de validade da sessão.
 - 2.1.1.5. Auditoria completa, com geração de logs e trilha de auditoria para cada acesso e uso de senha.
 - 2.1.1.6. Integração com diretórios LDAP, Active Directory e sistemas operacionais (Windows, Linux).
 - 2.1.1.7. Funcionalidade de acesso just-in-time (JIT) com autenticação multifator (MFA).
 - 2.1.1.8. Capacidade de escalabilidade para múltiplos cofre/usuário sem degradação de desempenho.

- 2.1.1.9. Módulo complementar de cofre pessoal para armazenamento seguro de senhas individuais e de uso sensível, não compartilhado, integrado a console principal da solução.
- 2.1.2. A solução deve permitir a segmentação por grupos, papéis e perfis de acesso, além de possibilitar a criação de políticas de expiração, complexidade e histórico de senhas. O Cofre deve estar integrado ao módulo de auditoria e gravação de sessões para rastreabilidade total dos acessos.
- 2.1.3. A solução deve ser capaz de identificar padrões suspeitos de uso de senhas, como tentativas de login fora do horário habitual, em dispositivos não reconhecidos ou com comportamento atípico, com geração de alertas em tempo real.
- 2.1.4. O cofre deverá permitir configurar se o usuário pode ou não visualizar a senha em texto claro, com base em perfis de acesso, tipo de credencial ou criticidade do sistema. Deve haver registro de cada visualização.
- 2.1.5. A ferramenta deve possibilitar o uso da credencial diretamente em uma sessão remota (via RDP/SSH/HTTPS) sem que o usuário visualize ou copie a senha, por meio de injeção de credencial (vault Injection).
- 2.1.6. O cofre deve realizar verificações periódicas de conformidade das credenciais armazenadas, com relação a políticas corporativas (tamanho, complexidade, periodicidade de troca etc.) e alertar desvios.
- 2.1.7. Deve haver mecanismo para exportação criptografada e controlada de um conjunto crítico de senhas, com proteção por senha de dupla custódia, para uso exclusivo em situações de falha total do sistema.
- 2.1.8. O cofre deve suportar backup periódico, criptografado e armazenado em repositório seguro, com opção de retenção e restauração para fins de recuperação de desastres e auditoria.
- 2.1.9. A solução deve garantir a imutabilidade das trilhas de auditoria (logs), com proteção contra alteração ou exclusão, de modo a assegurar evidência legal e forense de uso das credenciais.

2.2. Gerenciamento de Senhas

2.2.1. Funcionalidades gerais:

- 2.2.1.1. A solução deve permitir parametrização de políticas de segurança e força de senha pelo administrador do sistema, dentre as quais: conjunto de caracteres alfanuméricos, numéricos e caracteres especiais, podendo ser escolhidos também quais caracteres especiais serão permitidos, com possibilidade de não possibilitar caracteres repetidos, gerando senhas aleatórias;
- 2.2.1.2. Gerenciar chaves SSH e fazer Scan de servidores Linux e identificação e publicação de chaves SSH;
- 2.2.1.3. Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;
- 2.2.1.4. Consolidação periódica de senhas para identificar senhas que foram alteradas em sistemas gerenciados;
- 2.2.1.5. Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legados;
- 2.2.1.6. Oferecer interface com visão personalizada exclusiva para Auditorias e Órgãos Reguladores, contendo os dispositivos e credenciais gerenciadas pela solução;
- 2.2.1.7. Fornecer uma área de transferência segura, para que o solicitante possa visualizar ou copiar a senha na tela de login do sistema de destino;

- 2.2.1.8. A solução deve possibilitar o uso da credencial diretamente em uma sessão remota (RDP/SSH/HTTPS) por meio de injeção automática de credenciais (vault injeto), sem que o usuário visualize ou copie a senha. Opcionalmente, para cenários excepcionais, pode oferecer mecanismo controlado de visualização com registro de auditoria e limpeza automática;
- 2.2.1.9. Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata;
- 2.2.1.10. Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais;
- 2.2.1.11. Permitir o monitoramento on-line do uso das contas e desligamento da sessão;
- 2.2.1.12. Apresentar o recurso “break glass” para acesso de emergência às contas, ou seja, permitir acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas para as quais seria necessário aprovação em circunstâncias normais. Neste caso, os aprovadores e/ou administradores devem ser notificados imediatamente informando-os o motivo da emergência.
- 2.2.1.13. Oferecer a funcionalidade de “Discovery” para realizar busca de novos servidores, elementos de rede e banco de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos incluindo a possibilidade de descobrir certificados SSL;
- 2.2.1.14. Possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão caso o usuário execute um comando indevido;
- 2.2.1.15. Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;
- 2.2.1.16. Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiados;
- 2.2.1.17. Possibilidade de geração de relatórios baseados nos logs e exportá-los para arquivos em formato “.csv”;
- 2.2.1.18. A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, RPC, WinRM, SSH, API REST HTTP/HTTPS;
- 2.2.1.19. A solução deve permitir a criação de políticas de senhas de forma hierárquica ou em níveis de segurança, possibilitando a criação de senhas diferenciadas para grupos de ativos de diferentes de diferentes plataformas ou criticidades;
- 2.2.1.20. Possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de dupla custódia para recuperações de senhas no caso de falha total da solução;
- 2.2.1.21. A solução deve possibilitar políticas de senha que impeça visualização simultânea de credenciais, sessões, bem como também configurar o tempo de expiração das senhas baseadas por visualização e data de expiração. Também deve ser possível escolher dias específicos da semana e horários que as credenciais poderão expirar;
- 2.2.1.22. A solução deve ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos;
- 2.2.1.23. A solução não deverá depender da instalação de agentes para realizar a troca de senhas;
- 2.2.1.24. Checkout/Checkin de credencial: A solução deve redefinir a credencial (senha) no ambiente para os casos de visualização da senha pelo solicitante nos processos de checkout de credencial;
- 2.2.1.25. A solução deve ter a capacidade de realizar a reconciliação de credenciais automaticamente.

2.2.2. Rotação de senhas

- 2.2.2.1. Troca automática de senhas para Servidores (Unix, Linux, Windows), Bancos de Dados (MS SQL, ORACLE, MYSQL, PostgreSQL), Aplicações Web, Dispositivos de Rede, Mainframe;
- 2.2.2.2. Para execução de trocas de senhas, a solução deve permitir que o administrador configure a comunicação com aplicações e sistemas terceiros utilizando protocolos variados incluindo, no mínimo, RPC, WinRM, SSH, API REST HTTP/HTTPS;
- 2.2.2.3. As rotinas de execução de trocas de senha devem ser personalizáveis, de forma que um administrador possa alterar comandos a serem executados para que não seja necessário que se aguarde por uma nova atualização por parte do fabricante caso haja alguma alteração no sistema alvo;
- 2.2.2.4. As senhas geradas automaticamente pela solução de cofre de senhas devem seguir os seguintes requisitos:
 - 2.2.2.4.1. Poder determinar a quantidade de caracteres;
 - 2.2.2.4.2. Ser composta por números, letras maiúsculas, letras minúsculas e por caracteres especiais;
 - 2.2.2.4.3. Poder ser pré-definidas quais caracteres especiais poderão ser utilizados;
 - 2.2.2.4.4. Aleatórios de modo que dentro do histórico de uma conta seja improvável encontrar duas senhas iguais;
 - 2.2.2.4.5. Não seja baseada em palavra de dicionário.
 - 2.2.2.4.6. A solução deverá realizar a troca automática da senha da ligação entre servidores MS SQL Server com Linked Servers;
 - 2.2.2.4.7. Geração automática de senhas de força/complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa;
 - 2.2.2.4.8. Flexibilidade para configuração de força de senha gerada;
 - 2.2.2.4.9. Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;
 - 2.2.2.4.10. Possibilidade de gerenciar senhas privilegiadas em aplicações e interação com páginas web, tanto para sistemas externos e conhecidos, como para sistemas internos desenvolvidos por equipes internas;
 - 2.2.2.4.11. Armazenamento de histórico de senhas por equipamento;
 - 2.2.2.4.12. Registro de trocas executadas;
 - 2.2.2.4.13. Relatório de acompanhamento de trocas;
 - 2.2.2.4.14. Relatório de erros de trocas;
 - 2.2.2.4.15. Alertas de falha ou sucesso de trocas;
 - 2.2.2.4.16. Possibilidade de reconfiguração/customização de scripts ou plugin de troca de senhas para configuração de casos que exijam parâmetros específicos para rotação de senhas;
- 2.2.2.5. Configuração de políticas de trocas de senhas com agendamento programado ou por ocorrências de eventos com especificação de parâmetros de prazo para a troca;
- 2.2.2.6. Disponibilizar os Templates de troca de senha de forma que possam ser abertos, editáveis e auditáveis;
- 2.2.2.7. Rastreabilidade de Alteração de Template.

3. GERENCIAMENTO DE SISTEMAS, DISPOSITIVOS DE INFRAESTRUTURA E BANCO DE DADOS

3.1. Gerenciamento de Servidores

3.1.1. Do Controle de Acessos Privilegiados a Servidores

Serviço Nacional de Aprendizagem Comercial
Departamento Regional no Espírito Santo

Av. Marechal Mascarenhas de Moraes, 2077
Bento Ferreira - Vitória/ES - CEP 29050-935
Telefax: (27) 3325-8311 - www.es.senac.br

- 3.1.1.1. A solução de PAM deverá incluir um componente específico para o controle de acessos privilegiados a servidores físicos e virtuais, contemplando os seguintes requisitos:
- 3.1.1.2. Intermediação de sessões privilegiadas a servidores Windows, Linux e Unix por meio de jump server, sem a exposição de credenciais aos usuários.
- 3.1.1.3. Suporte a protocolos como RDP, SSH e outros utilizados para administração remota.
- 3.1.1.4. Aplicação de políticas de acesso com base em identidade, função e horário, com aprovação por workflow, se necessário.
- 3.1.1.5. Registro completo das sessões com gravação de vídeo, auditoria de comandos e geração de logs centralizados.
- 3.1.1.6. Integração nativa com cofre de senhas para extração e rotação automática de credenciais.
- 3.1.1.7. Capacidade de identificar e interromper sessões com comportamentos suspeitos em tempo real.
- 3.1.1.8. Suporte a acesso just-in-time (JIT), com autenticação multifator (MFA) e restrição por IP ou localidade.
- 3.1.1.9. Interface administrativa centralizada para delegação de permissões e visualização de sessões ativas e passadas.
- 3.1.1.10. Este componente deve garantir a rastreabilidade e a conformidade com normas de segurança e auditoria, reduzindo o risco de mau uso de credenciais privilegiadas em ambientes críticos de infraestrutura.

3.2. Gerenciamento de Dispositivos de Rede

3.2.1. Do Controle e Auditoria de Acessos a Dispositivos de Rede

- 3.2.1.1. A solução PAM deverá incluir um componente específico para o gerenciamento de acessos privilegiados a dispositivos de rede, tais como switches, roteadores, firewalls e balanceadores de carga, com os seguintes requisitos mínimos:
- 3.2.1.2. Intermediação de sessões administrativas via SSH, Telnet ou protocolos compatíveis, sem exposição das credenciais aos usuários.
- 3.2.1.3. Integração com o cofre de senhas para extração segura de credenciais e rotação periódica automática.
- 3.2.1.4. Registro completo das sessões com auditoria de comandos executados e exportação de logs para ferramentas SIEM.
- 3.2.1.5. Aplicação de políticas de acesso baseadas em perfis, horários, grupos de usuários e tipos de dispositivo.
- 3.2.1.6. Suporte a workflows de aprovação para acesso a dispositivos críticos ou fora do horário padrão.
- 3.2.1.7. Capacidade de bloquear ou encerrar sessões em tempo real com base em comportamento suspeito ou não autorizado.
- 3.2.1.8. Compatibilidade com equipamentos dos principais fabricantes do mercado.
- 3.2.1.9. Relatórios detalhados de auditoria e conformidade com requisitos regulatórios e melhores práticas de segurança.
- 3.2.1.10. Esse componente deve garantir a rastreabilidade, controle e proteção de infraestruturas críticas, reduzindo o risco de falhas humanas, configurações indevidas e acessos indevidos em dispositivos essenciais da rede corporativa.

3.3. Gerenciamento de Sistemas e Aplicações

3.3.1. A solução de PAM deverá contemplar a funcionalidade para gerenciamento seguro de acessos privilegiados a sistemas e aplicações críticas da organização, tais como ERPs, CRMs, sistemas web internos, painéis administrativos, sistemas legados e consoles de gerenciamento, garantindo controle, rastreabilidade e proteção das credenciais utilizadas.

3.3.1.1. Os requisitos mínimos incluem:

3.3.1.1.1. Intermediação de sessões privilegiadas a sistemas via navegador (browser-based) ou através de conectores próprios, sem exposição de senhas ao usuário.

3.3.1.1.2. Compatibilidade com aplicações que utilizam autenticação web (form-based, SSO, SAML, Kerberos), consoles desktop (como o SmartConsole), ou APIs para acesso programático.

3.3.1.1.3. Integração com o Cofre de Senhas para extração, rotação e injeção automática de credenciais durante a abertura da sessão.

3.3.1.1.4. Registro detalhado das atividades realizadas dentro da aplicação, com captura de vídeo da sessão, geração de logs e marcação de ações críticas.

3.3.1.1.5. Possibilidade de configurar workflows de aprovação para acesso a sistemas sensíveis com definição de janelas de acesso, restrições por IP, horário e perfil de usuário.

3.3.1.1.6. Suporte a autenticação multifator (MFA) para acesso à plataforma PAM e aos sistemas acessados, aplicando o princípio de zero trust.

3.3.1.1.7. Bloqueio ou encerramento automático de sessões que apresentem comportamentos anômalos ou não autorizados.

3.3.1.1.8. Integração com sistemas legados ou proprietários via scripts, comandos, macros ou chamadas API, respeitando padrões de segurança e segregação.

3.3.1.1.9. Capacidade de aplicar políticas de acesso distintas por tipo de sistema, nível de criticidade ou sensibilidade da aplicação.

3.3.1.1.10. Relatórios específicos por aplicação acessada, com trilha de auditoria, controle de tempo de uso, ações realizadas e identificação do responsável pelo acesso.

3.4. Gerenciamento de Banco de Dados

3.4.1. A solução PAM deverá contemplar a funcionalidade ao gerenciamento seguro e auditável de acessos privilegiados a bancos de dados, garantindo controle, rastreabilidade e proteção das credenciais utilizadas por administradores, desenvolvedores, analistas e sistemas automatizados.

3.4.1.1. Os requisitos mínimos incluem:

3.4.1.1.1. Intermediação de acessos administrativos a bancos de dados (ex.: MS SQL Server, Oracle, MySQL, PostgreSQL, DB2, MongoDB etc.) sem exposição das credenciais ao usuário.

3.4.1.1.2. Suporte à injeção segura de credenciais diretamente nas sessões SQL via ferramentas de administração (SQL Management Studio, Oracle SQL Developer, DBeaver, etc.).

3.4.1.1.3. Integração com Cofre de Senhas para extração e rotação automática de senhas de contas administrativas e de serviço em bancos de dados.

3.4.1.1.4. Registro completo das sessões com captura de comandos SQL executados, geração de logs, alertas e exportação para SIEM.

3.4.1.1.5. Aplicação de políticas de acesso com base em função, sistema, horário, perfil e criticidade do banco de dados, com aprovação via workflow quando necessário.

3.4.1.1.6. Suporte ao acesso just-in-time (JIT), com janela de tempo limitada e autenticação multifator (MFA) para acesso.

- 3.4.1.1.7. Detecção de comandos perigosos ou ações indevidas, com possibilidade de bloqueio ou encerramento automático da sessão.
- 3.4.1.1.8. Rastreabilidade total com trilha de auditoria detalhada de quem acessou qual banco, quando, por quanto tempo, com quais permissões e quais ações foram executadas.
- 3.4.1.1.9. Capacidade de descoberta automatizada de instâncias de banco de dados e contas privilegiadas associadas.
- 3.4.1.1.10. Suporte à rotação de senhas de Linked Servers em ambientes Microsoft SQL Server e equivalentes em outros SGBDs.
- 3.4.1.1.11. Interface administrativa centralizada para gestão de políticas, permissões, relatórios e auditoria de acessos a bancos de dados.
- 3.4.1.1.12. Compatibilidade com conexões por protocolos como ODBC, JDBC, TDS, e suporte a execução de scripts customizados de rotação e acesso.

4. ACESSO REMOTO PRIVILEGIADO

4.1. Especificações gerais

- 4.1.1. A solução deve possuir funcionalidade que permita a conexão segura de usuários por intermédio da Internet, sem necessidade de uso de VPN;
- 4.1.2. O acesso privilegiado remoto deve ser realizado por meio de um gateway seguro do Fabricante;
- 4.1.3. O gateway de acesso remoto do fabricante deve ser no Brasil, de forma a manter o desempenho nos acessos remotos;
- 4.1.4. O acesso remoto deve ser realizado por meio do navegador, utilizando sessão SSL;
- 4.1.5. Todos os recursos da solução de gerenciamento de acesso, como gravação de sessão, acompanhamento em tempo real, bloqueio de comandos e análise de comportamento, devem estar disponíveis para sessões remotas.

4.2. Acesso de usuários internos (colaboradores)

- 4.2.1. A solução deve permitir que usuários internos cadastrados na solução possam acessar a mesma interface de gerência, utilizando o acesso remoto seguro;
- 4.2.2. Os usuários internos devem usar a mesma forma de autenticação para acesso remoto que utilizam quando acessam diretamente a solução, incluindo o uso de MFA;
- 4.2.3. Deve ser possível configurar a duração da liberação de acesso externo para usuários internos.
- 4.2.4. O acesso de usuários internos deverá ser intermediado pela solução PAM, com total segregação de credenciais e sem exposição de senhas em nenhum momento durante a sessão.
- 4.2.5. Os usuários internos devem utilizar os mesmos mecanismos de autenticação forte para acesso remoto, exigindo autenticação multifator (MFA), com suporte a token, aplicativo autenticador, biometria ou integração com soluções de identidade corporativa (ex: Azure AD, ADFS, SAML, LDAP).
- 4.2.6. A solução deve permitir a definição de regras específicas de autorização para usuários internos, considerando:
 - 4.2.6.1. Perfis e funções (ex.: administrador, analista, suporte);
 - 4.2.6.2. Critérios contextuais como horário, endereço IP, localização geográfica ou VLAN;
 - 4.2.6.3. Tipo de ativo a ser acessado (servidores, bancos, dispositivos de rede etc.).
- 4.2.7. Deve ser possível configurar a duração do acesso remoto por tempo determinado, com base em políticas pré-definidas (ex: 30 minutos, 2 horas), e incluir aprovação por workflow em casos críticos.

- 4.2.8. Toda sessão realizada por usuários internos deve ser gravada em vídeo e possuir trilha de auditoria detalhada (comandos, tempo, IP de origem, justificativa, ativos acessados).
- 4.2.9. A solução deve oferecer visibilidade em tempo real sobre as sessões ativas realizadas por usuários internos, com possibilidade de intervenção manual ou automatizada, em caso de comportamento suspeito.
- 4.2.10. Deve permitir a configuração de alertas e notificações automáticas para os gestores responsáveis, sempre que um usuário interno iniciar uma sessão privilegiada fora da política normal de operação.
- 4.2.11. O sistema deve manter logs completos para fins de auditoria e conformidade, com exportação para soluções de SIEM e geração de relatórios detalhados por usuário, ativo, grupo ou data.

4.3. Acesso de usuários externos (terceiros)

- 4.3.1. A solução PAM deverá oferecer funcionalidades para o gerenciamento seguro, controlado e auditável do acesso privilegiado por terceiros, tais como fornecedores, prestadores de serviço, consultorias, suporte técnico remoto e equipes externas que necessitem acessar recursos críticos da infraestrutura organizacional. O acesso por terceiros representa um vetor de risco elevado e, por isso, requer controles mais rigorosos de autorização, supervisão e rastreamento.

4.3.2. Acesso Segregado para Terceiros

- 4.3.2.1. A plataforma deve permitir o provisionamento de contas específicas para terceiros, com segregação de ambiente e permissões mínimas necessárias para o desempenho das atividades contratadas. Funcionalidades exigidas que reduz o risco de acesso indevido e facilita o rastreamento da atuação de cada fornecedor:
 - Criação de perfis dedicados para terceiros, separados dos usuários internos.
 - Definição de escopo de acesso baseado em contratos, SLAs ou tempo de atividade.
 - Restrições por sistemas, grupo de ativos, OU do AD ou VLAN.

4.3.3. Autenticação e Autorização Fortes

- 4.3.3.1. O sistema deve aplicar mecanismos rigorosos de autenticação e autorização para o acesso de terceiros ao ambiente PAM. Funcionalidades exigidas para elevar o nível de segurança no acesso remoto por atores externos à organização:
 - Autenticação multifator (MFA) obrigatória para usuários externos.
 - Possibilidade de integração com sistemas de identidade federada (ex.: SAML, LDAP, Azure AD B2B).
 - Autorização com base em papéis, perfis e tempo de acesso.

4.3.4. Acesso Just-in-Time (JIT) para Terceiros

- 4.3.4.1. O acesso de terceiros deverá seguir o princípio do acesso temporário sob demanda (JIT), com concessão limitada e controlada. Funcionalidades exigidas para garantir o princípio do mínimo privilégio e reduz drasticamente a exposição contínua de contas privilegiadas:
 - Liberação de acesso somente mediante solicitação justificada e aprovação.
 - Acesso temporário com janela de tempo definida (ex.: 1 hora, 1 dia).
 - Expiração automática após o uso ou término do período.
 - Possibilidade de restrição por IP, localização ou dispositivo.

4.3.5. Workflows de Aprovação Específicos para Terceiros

- 4.3.5.1. A solução deverá permitir a configuração de fluxos de aprovação personalizados para acesso de terceiros, com diferentes níveis de autorização, notificações e controle. Funcionalidades

exigidas para assegurar responsabilidade compartilhada e documentação completa sobre o porquê e por quem o acesso foi concedido:

- Solicitação formal de acesso com justificativa, data e duração.
- Aprovação por responsáveis técnicos ou gestores da área requisitante.
- Registro do responsável pela autorização e da finalidade do acesso.
- Encaminhamento automático de alertas ou rejeições.

4.3.6. Sessão Monitorada e Gravação de Acesso

4.3.6.1. Durante a sessão remoto de terceiros, a ferramenta deve permitir monitoramento em tempo real e gravação das atividades executadas. Funcionalidades exigidas para fornecer evidência para auditorias, investigação de incidentes e prevenção de comportamentos maliciosos.

- Captura de vídeo da sessão (screen recording).
- Visualização em tempo real com possibilidade de intervenção ou encerramento.
- Geração de trilhas de auditoria com comandos, janelas acessadas e tempo de atividade.
- Classificação e marcação de eventos suspeitos na gravação.

4.3.7. Acesso sem Exposição de Senhas (Passwordless / Vault Injection)

4.3.7.1. A solução deve permitir que terceiros acessem de forma segura sem visualizar ou digitar senhas, utilizando técnicas como injeção de credenciais diretamente na sessão. Funcionalidades exigidas para minimizar o risco de vazamento ou reutilização indevida de credenciais críticas por fornecedores:

- Lançamento de sessão remota com credencial injetada automaticamente.
- Proibição de exibição de senha em texto claro.
- Sessões RDP, SSH ou Telnet com credenciais sigilosas geridas pelo cofre de senhas.

4.3.8. Auditoria e Rastreabilidade Total de Terceiros

4.3.8.1. Todo acesso realizado por terceiros deve ser completamente rastreável, com geração de logs detalhadas e relatórios de conformidade. Funcionalidades exigidas para proporcionar visibilidade total e facilitar a prestação de contas e a conformidade com exigências legais e contratuais:

- Registro de acesso com dados como: quem, quando, onde, por quanto tempo, o que fez e por qual motivo.
- Exportação de relatórios para auditoria externa e governança interna.
- Relatórios customizáveis por fornecedor, contrato, sistema acessado ou tempo de atividade.

4.3.9. Revogação imediata de Acesso

4.3.9.1. A ferramenta deve permitir a revogação imediata e remota do acesso concedido a terceiros, com aplicação de medidas de segurança adicionais em caso de incidentes. Funcionalidades exigidas para permitir resposta rápida a riscos emergentes e previne o uso contínuo indevido de privilégios.

- Bloqueio manual ou automático de conta de terceiros.
- Encerramento de sessões ativas.
- Revogação de tokens de autenticação ou senhas temporárias.
- Notificação ao gestor responsável.

4.3.10. Integração com Contratos e Termos de Responsabilidade

4.3.10.1. A solução deve permitir vincular o acesso de terceiros a contratos, termos de confidencialidade e regras de uso previamente definidos. Funcionalidade exigidas para garantir conformidade contratual e legal, além de reforçar a responsabilização do fornecedor.

- Registro do aceite do Termo de Responsabilidade e Confidencialidade e regras de uso previamente definidos.
- Upload de documentos associados à conta do fornecedor.
- Registro de vigência do contrato e bloqueio automático após expiração.

5. ELEVAÇÃO DE PRIVILÉGIOS

5.1. Especificações gerais

- 5.1.1. A solução deverá permitir a elevação granular de privilégios para aplicações específicas, sem a necessidade de conceder privilégios administrativos permanentes ao usuário.
- 5.1.2. A solução deverá permitir a elevação temporária de privilégios para execução de aplicações, mediante políticas previamente definidas.
- 5.1.3. A solução deverá suportar controle de execução de aplicações baseado em políticas, incluindo mecanismos de whitelist e blacklist.
- 5.1.4. A solução deverá permitir a elevação controlada de funcionalidades administrativas do sistema operacional, incluindo itens do painel de controle e ferramentas administrativas.
- 5.1.5. A solução deverá permitir a segregação de permissões administrativas, possibilitando que diferentes grupos de usuários tenham acesso apenas a funcionalidades específicas do sistema.
- 5.1.6. A solução deverá permitir o controle e gerenciamento da execução de aplicações instaladas, incluindo políticas de autorização ou bloqueio.
- 5.1.7. A solução deverá possuir funcionamento em modo offline, mantendo um cache seguro de políticas previamente definidas, permitindo a aplicação das regras mesmo em caso de indisponibilidade do servidor central.
- 5.1.8. A solução deverá possuir mecanismos para redução de riscos de movimentação lateral, incluindo controle sobre ferramentas administrativas, conexões remotas e execução de utilitários do sistema.
- 5.1.9. A solução deverá permitir o controle de execução de processos filhos, garantindo que aplicações elevadas não possam iniciar outros processos não autorizados.
- 5.1.10. A solução deverá permitir a definição de prazos de validade para permissões concedidas, facilitando o controle de acessos temporários, especialmente para usuários terceiros.
- 5.1.11. A solução deverá permitir a gravação e auditoria das sessões de elevação de privilégio, possibilitando rastreabilidade das ações realizadas.
- 5.1.12. A solução deverá permitir configuração granular de quais aplicações ou processos terão suas sessões registradas.
- 5.1.13. A solução deverá registrar logs detalhados das execuções de aplicações e eventos de elevação de privilégio, armazenando-os em repositório centralizado para fins de auditoria.
- 5.1.14. A solução deverá permitir integração com plataformas externas de análise de risco ou reputação de arquivos, auxiliando na validação de executáveis antes de sua execução.
- 5.1.15. Todas as execuções de aplicações e eventos relacionados à elevação de privilégios deverão ser registradas e disponibilizadas em relatórios centralizados, com possibilidade de filtros por usuário, dispositivo, aplicação ou tipo de evento.
- 5.1.16. A solução deverá permitir controle granular de permissões administrativas da própria plataforma, possibilitando segregação de funções entre administradores, auditores e operadores.

- 5.1.17. A solução deverá permitir a execução de ações administrativas específicas utilizando credenciais privilegiadas controladas pela plataforma, sem exposição direta das credenciais ao usuário final.
- 5.1.18. O licenciamento referente à funcionalidade de elevação de privilégios deverá ser precificado considerando o quantitativo de 15 (quinze) licenças
- 5.1.19. Para fins de composição de proposta comercial, a CONTRATADA deverá utilizar como base os itens 5 e 6 da tabela de preços, garantindo a correta correspondência dos valores apresentados para esta funcionalidade.

6. CADASTRAMENTO DE DISPOSITIVOS E CREDENCIAIS

6.1. Cadastramento de dispositivos

- 6.1.1. A solução deve possibilitar o cadastro de equipamentos através de, pelo menos:
 - 6.1.1.1. Cadastro manual;
 - 6.1.1.2. Cadastro em lote via planilha;
 - 6.1.1.3. Discovery/Scan de dispositivos.
- 6.1.2. A solução deve permitir o cadastro de novos valores para atributos que definem o dispositivo, como Fabricante, Modelo, Tipo de Dispositivo etc.;
- 6.1.3. A solução deve possibilitar a associação de tags aos dispositivos, para que a segregação de acesso e a geração de relatórios possa ser organizada da melhor forma.

6.2. Descoberta de dispositivos e credenciais

- 6.2.1. A solução deve ser capaz de encontrar dispositivos de rede e credenciais, de no mínimo os seguintes ambientes:
 - 6.2.1.1. Servidores Linux/Unix, Windows e VMWare;
 - 6.2.1.2. Base de dados Oracle, SQL e MySQL;
 - 6.2.1.3. Dispositivos de rede como firewalls, roteadores, switches e balanceadores;
 - 6.2.1.4. Workstation.
- 6.2.2. A solução deve ser capaz de fazer a descoberta em domínios, encontrando dispositivos e credenciais em Active Directory;
- 6.2.3. A solução deve possuir integração nativa ou por meio de API com plataformas DevOps como Kubernetes, Openshift, Docker, Ansible, Jenkins, Terraform e GitLab, permitindo o gerenciamento seguro de segredos (secrets), chaves de API, tokens e credenciais utilizados nesses ambientes.
- 6.2.4. A solução deve realizar a descoberta de contas de serviço Windows, além de identificar quais dispositivos que estão utilizando a conta;
- 6.2.5. A solução deve possuir um dashboard ou relatório que liste o andamento da execução dos discoveries, incluindo sua barra de progresso;
- 6.2.6. A solução deve ser capaz de realizar um escaneamento contínuo nos dispositivos, trazendo informações de acessos suspeitos ou indevidos, como por exemplo, acesso ao dispositivo com credenciais que não estejam cadastradas no cofre, ou o acesso que foi por fora da solução PAM;
- 6.2.7. A solução deve ser capaz de realizar a descoberta, armazenamento e gestão automática de chaves SSH em sistemas Linux;
- 6.2.8. A solução deve possibilitar uma descoberta contínua, ou seja, deve ser possível cadastrar dias e horários para a reexecução de uma descoberta, incluindo a seleção de períodos e dias que serão executados.

6.3. Gerenciamento De Sessões

- 6.3.1. A solução de permitir o gerenciamento e monitoramento de sessões estabelecidas via protocolos: HTTP, HTTPS, SSH e RDP, seja via navegador ou client externo;
- 6.3.2. A solução deve permitir monitoramento em tempo real das sessões ou atividades dos usuários privilegiados, disponibilizada em interface centralizada (Dashboard);
- 6.3.3. A solução deve garantir o monitoramento das atividades realizadas com contas de acesso privilegiado obtidas de forma emergencial (“break-glass”);
- 6.3.4. A solução deve possuir funcionalidade de gravação das sessões dos usuários privilegiados;
- 6.3.5. A gravação de sessão de usuário deve suportar a gravação contínua de toda a sessão em vídeo;
- 6.3.6. A gravação de sessão deve possibilitar o registro da interação do mouse e teclado durante a sessão;
- 6.3.7. A solução deve suportar a gravação da sessão de usuários simultâneos. A quantidade máxima de sessões deve ser baseada no hardware utilizado para a solução, não tendo limitação de software;
- 6.3.8. As gravações de sessão devem ser armazenadas em formato criptografado;
- 6.3.9. A solução deve possibilitar o gerenciamento e monitoramento de sessões privilegiadas a portais web acessados via browser, como consoles de cloud, interfaces web de ativos de rede, e até mesmo redes sociais corporativas;
- 6.3.10. A solução não deverá depender da instalação de agentes para realizar a gravação de sessão;
- 6.3.11. Gravação de comandos digitados em ambientes RDP e SSH;
- 6.3.12. Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download;
- 6.3.13. Exportação de sessão em formato vídeo;
- 6.3.14. Busca de registro de sessão por usuário, sistema alvo, IP de origem, data e hora;
- 6.3.15. Busca por comandos e entradas de teclado digitados em sessões SSH;
- 6.3.16. Busca de comandos e entradas de teclado em CMD e Powershell executados em sessões RDP;
- 6.3.17. Tecnologia de Optical Character Recognition (OCR) para indexação de textos encontrados em gravações de sessão;
- 6.3.18. Armazenamento e consulta de logs que forneçam aos menos, as seguintes informações:
 - 6.3.18.1. Identificação do usuário que realizou determinado acesso a um dispositivo;
 - 6.3.18.2. Identificação de quem aprovou o acesso do usuário;
 - 6.3.18.3. Data e hora do acesso realizado.
- 6.3.19. Permitir o acompanhamento ao vivo de sessões remotas pelo administrador e desligamento da sessão remotamente;
- 6.3.20. A solução deve permitir configuração de fluxo de aprovação para consultas de senhas e início de sessões;
- 6.3.21. A solução deve permitir que seja configurado para que o segundo fator de autenticação seja revalidado ao iniciar-se uma sessão.
- 6.3.22. Controle de acesso
 - 6.3.22.1. A solução deve ser capaz de limitar a execução de comandos críticos pelos usuários cadastrados;
 - 6.3.22.2. A solução deve permitir o controle de execução de comandos críticos por “lista de aprovação” e/ou “lista de negação”;
 - 6.3.22.3. A solução deve permitir o início e a condução de sessões dentro do próprio navegador, dispensando o uso de clientes externos como o mstsc.exe e o putty.exe;

- 6.3.22.4. A solução deve possuir tempo de expiração de sessão por ociosidade configurável pelo administrador do sistema;
- 6.3.22.5. A solução deve permitir a parametrização do número máximo de sessões ativas por usuário;
- 6.3.22.6. A solução deve suportar a desconexão da sessão por atividade/uso indevido de comandos pré-cadastrados no sistema;
- 6.3.22.7. A solução deve permitir a criação de grupos de usuários;
- 6.3.22.8. Controle de comando com alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução – Baseado em listas de permissão e listas de negação;
- 6.3.22.9. Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;
- 6.3.22.10. Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;
- 6.3.22.11. Marcação de pontuação de comandos de acordo com nível de risco de cada comando;
- 6.3.22.12. A solução deve permitir a atribuição de privilégios a grupos de usuários, associados a um ou mais alvos gerenciados;
- 6.3.22.13. A solução deve permitir integração com ferramenta de gestão de incidentes (ITSM) para validade tickets abertos durante processo de aprovação de acesso;
- 6.3.22.14. A solução deve permitir acesso simultâneo ao cofre de senhas e as contas privilegiadas por dois ou mais usuários;
- 6.3.22.15. A solução deve possibilitar a concessão de acesso a credenciais diferentes para usuários diferentes, mesmo que sejam usadas para acessar o mesmo dispositivo;
- 6.3.22.16. A solução deve possibilitar a segregação de acesso a credenciais e dispositivos baseadas em tags;
- 6.3.22.17. A solução deve fornecer funcionalidade para revogar imediatamente todas as sessões remotas para um usuário conectado;
- 6.3.22.18. Acessos simultâneos a credenciais, senhas e dispositivos não devem possuir comprometimento da rastreabilidade.
- 6.3.22.19. Gerenciamento de sessões em bancos de dados
- 6.3.22.20. A solução deverá gerenciar de forma segura e auditada as sessões privilegiadas para os bancos de dados, SQL server, Oracle e PostgreSQL, com o mínimo os seguintes requisitos técnicos:
- 6.3.22.21. Deverá prover a sessão ao dispositivo final de forma transparente, segura, gravada e auditada sem a necessidade de instalar agentes do fabricante ou terceiros;
- 6.3.22.22. Deverá realizar a verificação em tempo real dos comandos e query, tendo a inteligência e funcionalidade de realizar minimamente as seguintes ações: bloqueio de execução quando não permitido pela solução, encerramento da sessão e envio de notificação/alerta de riscos aos DBAs, quando configurados e identificados pela solução;
- 6.3.22.23. Deverá possuir tecnologia que registre e armazene todas as atividades realizadas através da solução para fins de auditoria e consulta posterior;
- 6.3.22.24. Deverá possuir a customização do privilégio do acesso por usuário, grupo de usuário e dispositivo, via interface centralizada de administração da solução;
- 6.3.22.25. O proxy de banco de dados deve permitir o acesso por intermédio do aplicativo padrão do SGBD, mantendo todo o controle e auditoria de sessão descritas nesta Especificação Técnica.
- 6.3.23. Automação de tarefas privilegiadas

- 6.3.23.1. A solução deverá realizar a execução de tarefas com scripts pré-cadastrados, podendo ser possível escolher múltiplos dispositivos para um mesmo script;
- 6.3.23.2. As tarefas devem ser executadas em dispositivos gerenciados através de, pelo menos, os protocolos SSH, RPC, WinRM, LDAPS;
- 6.3.23.3. Automações de interações com páginas web também ser executadas em forma de tarefas;
- 6.3.23.4. A solução deverá possuir workflow de aprovação para a execução de tarefas, incluindo aprovação multinível com pelo menos 3 níveis;
- 6.3.23.5. A solução deve possibilitar a criação de variáveis para execução, sendo definidos os nomes das variáveis e o valor dela, como por exemplo ao cadastrar o script: echo 'VARIÁVEL', a execução será echo 'valor variável';
- 6.3.23.6. A solução deverá possuir relatórios com o histórico de execuções, indicando qual script executado, em quais dispositivos, se houve erro e quem foi o solicitante;
- 6.3.23.7. A solução deve ter a capacidade de programar a execução das tarefas para um horário determinado.

7. DOS SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

7.1. Funcionalidades gerais

- 7.1.1. O serviço de instalação e configuração da ferramenta adquirida já está incluída no escopo da contratação e deve ser realizado pela CONTRATADA.
- 7.1.2. A CONTRATADA deverá realizar a instalação dos módulos contratados no prazo máximo de 30 (trinta) dias, após a assinatura do contrato;
- 7.1.3. Deverá ser fornecido relatórios de Pré-Requisitos de Instalação e Operações dos Produtos, contendo, por produto, informação de todos os seus pré-requisitos de instalação e operação, a citar: todas conexões físicas e lógicas, e configuração do appliance necessárias para interligação da solução com o ambiente proposto pela CONTRATANTE;
- 7.1.4. Deverá ser efetuado levantamento de requisitos, coletando-se informações do ambiente computacional do CONTRATANTE, por meio de reuniões e verificações in-loco, com o objetivo de documentar e analisar informações quanto aos componentes de infraestrutura bem como estabelecer os parâmetros necessários à configuração e integração da solução;
- 7.1.5. A CONTRATADA deverá prestar consultoria para implantar toda a solução de acordo com as melhores práticas da indústria de TI, alocando profissionais devidamente capacitados e dentro dos níveis dos serviços contratados pelo órgão;
- 7.1.6. Deverá ser realizada configuração básica de designação de IP para acesso a solução adquirida para possibilitar a realização dos serviços de configuração das funcionalidades exigidas neste termo de referência;
 - 7.1.6.1. Plano de configuração:
 - 7.1.6.1.1. Diagrama de interconexão da solução;
 - 7.1.6.1.2. Projeto lógico de configuração;
 - 7.1.6.1.3. Configuração da solução;
 - 7.1.6.2. Plano de Execução:
 - 7.1.6.2.1. Cronograma de atividades;
 - 7.1.6.2.2. Responsáveis técnicos pelas atividades;
 - 7.1.6.3. Planos de Testes.
- 7.1.7. A CONFIGURAÇÃO deverá ser agendada junto à equipe técnica do CONTRATANTE com antecedência mínima de 48 (quarenta e oito) horas e respeitar o cronograma entregue;

- 7.1.8. As atividades de instalação dos equipamentos deverão ocorrer, preferencialmente, em dias úteis, no período das 09h às 22h, horário do local da instalação;
- 7.1.8.1.1. Caso a configuração possa provocar indisponibilidade nos serviços, a instalação poderá ocorrer em horário noturno e/ou fim de semana, a critério do CONTRATANTE;
- 7.1.9. Os procedimentos envolvidos nos processos de configuração deverão ser previamente aprovados pelo CONTRATANTE;
- 7.1.10. Após a configuração deverá ser agendado a execução do plano de testes para demonstrar efetividade das configurações realizadas e funcionamento de cada característica da Solução adquirida.

8. DA GARANTIA DO FABRICANTE PELO PERÍODO DE 12 MESES

8.1. Requisitos gerais

- 8.1.1. Todas as licenças deverão ser emitidas pelo Fabricante, com respectivos pacotes de atualização e garantia, incluindo:
 - 8.1.1.1. Atualização de versão;
 - 8.1.1.2. Suporte técnico do fabricante;
 - 8.1.1.3. Disponibilização de patches corretivos.
- 8.1.2. O licenciamento da solução deverá ser no modelo de subscrição (subscription), compatível com o modelo SaaS solicitado, garantindo que durante toda a vigência do contrato o SENAC ES tenha direito a atualizações de versão, patches de segurança, suporte técnico do fabricante e acesso contínuo a todas as funcionalidades contratadas. Ao término do contrato, os dados do SENAC ES deverão ser exportáveis em formato aberto ou estruturado;
- 8.1.3. Todos os produtos deverão ser fornecidos em sua versão/release mais recente;
- 8.1.4. A cada nova versão, a CONTRATADA deverá fornecer manuais de uso atualizados da solução, caso existam;
- 8.1.5. ACONTRATANTE deverá ter como opção executar ou não as atualizações de softwares disponibilizados.
- 8.1.6. Além da atualização de versão, a garantia do fabricante inclui os serviços de suporte e manutenção;
- 8.1.7. Os serviços de suporte e manutenção poderão ser prestados pela CONTRATADA ou por representante indicada pela CONTRATADA ou pelo fabricante da solução, sem prejuízo a responsabilidade integral da CONTRATADA quanto aos atendimentos dos níveis de serviço;
- 8.1.8. Entende-se por “suporte e manutenção”, doravante denominada unicamente como “Suporte”, toda atividade do tipo “corretiva”, não periódica, que variavelmente poderá ocorrer, durante todo o período de garantia. Possui suas causas em falhas e erros no software/hardware e trata da correção dos problemas atuais e não iminentes de sua fabricação.
- 8.1.9. Esse “Suporte” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:
 - 8.1.9.1. DO Software: desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados;
 - 8.1.9.2. Quanto às atualizações pertinentes aos softwares: entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando

inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia do contrato.

8.1.10. A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de software (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objetivo do contrato.

8.1.10.1. O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software.

8.1.11. É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de “Suporte” do tipo “preventiva” que pela sua natureza reduza a incidência de problemas que possam gerar “Suporte” do tipo “corretiva”. As manutenções do tipo “preventiva” não podem gerar custos a CONTRATANTE;

8.1.12. A manutenção técnica do tipo “corretiva” será realizada sempre que solicitado pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a outra informada pela CONTRATADA) via telefone (com número do tipo “0800”) ou Internet ou e-mail ou fac-símile ou outra forma de contato;

8.1.13. Os serviços de “Suporte” incluem:

8.1.13.1. Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação e desenvolvimento;

8.1.13.2. Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;

8.1.13.3. Esclarecimento de dúvidas sobre o funcionamento e operação da solução;

8.1.13.4. Instalação de novas versões ou atualizações e patches, quando disponibilizados pelo Fabricante;

8.1.14. A CONTRATADA deve disponibilizar a central de atendimento 24 horas por dia, 7 dias por semana (incluindo feriados) e equipe com conhecimentos sólidos no funcionamento e operação da solução de gestão.

8.1.15. Os prazos para a prestação dos serviços devem garantir a observância ao atendimento do seguinte Acordo de Níveis de Serviços (ANS) e sua SEVERIDADE.

Severidade	Prazo de início de atendimento	Prazo de resolução
Urgente/Crítico	02 horas	12 horas
Importante	04 horas	24 horas
Normal	08 horas	36 horas
Informação	12 horas	48 horas

8.1.15.1. Os prazos são contados em horas úteis, considerando a jornada de trabalho das 08:00h às 18:00h;

8.1.15.2. Descrição das severidades para categorização dos chamados:

8.1.15.2.1. SEVERIDADE URGENTE/CRÍTICO: Solução totalmente inoperante, casos em que o ambiente se encontra paralisado e nenhuma solução alternativa está disponível para ser aplicada. Os usuários estão impossibilitados de fazer login na solução e possuir acesso às credenciais gerenciadas pela ferramenta. Incidentes/problemas em geral que prejudicam fortemente a operação da organização e suas tarefas diárias;

8.1.15.2.2. SEVERIDADE IMPORTANTE: Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução;

- 8.1.15.2.3. SEVERIDADE NORMAL: Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução;
- 8.1.15.2.4. SEVERIDADE INFORMAÇÃO: Solicitações de informações diversas ou dúvidas sobre a solução.
- 8.1.15.3. Em caso de problemas com a Solução, fruto de falha de elemento de hardware e/ou software não fornecido pela CONTRATADA, os tempos de atendimento são pausados até a resolução do problema por parte da CONTRATANTE ou equipe indicada.
- 8.1.16. Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde ele está instalado;
- 8.1.17. Na abertura de chamados técnicos, serão fornecidas informações, como número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e severidade do chamado;
- 8.1.18. A severidade do chamado poderá ser reavaliada quando verificado que ela foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;
- 8.1.19. A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento.

9. DO SERVIÇO DE REPASSE DE CONHECIMENTO

9.1. Do repasse de conhecimento

- 9.1.1. Durante a instalação e configuração dos módulos contratados, a CONTRATADA, deverá realizar o repasse de conhecimento para a equipe do SENAC ES envolvida no projeto;
- 9.1.2. O repasse deverá ser realizado no ambiente do SENAC ES ou disponibilizado pela CONTRATADA, com duração mínima de 20 (vinte) horas, pelo analista responsável pela instalação e configuração da solução;
- 9.1.3. A formação deve contemplar tanto aspectos conceituais quanto práticos, abordando tópicos como:
- 9.1.3.1. Arquitetura da solução e seus componentes;
- 9.1.3.2. Instalação e configuração dos módulos adquiridos;
- 9.1.3.3. Integrações com o ambiente do SENAC ES (AD, servidores, redes etc.);
- 9.1.3.4. Operação diária (inclusão de ativos, políticas, senhas, usuários etc.);
- 9.1.3.5. Monitoramento e análise de registros (logs, alertas, auditorias);
- 9.1.3.6. Resolução de problemas comuns (troubleshooting básico);
- 9.1.3.7. Atualização e manutenção da solução (patches, upgrades, backups);
- 9.1.3.8. Procedimentos de resposta a incidentes com apoio da ferramenta.
- 9.1.4. Deverá ser fornecido material didático completo e em português, contendo:
- 9.1.4.1. Manual do administrador (admin guide);
- 9.1.4.2. Manual de operação do sistema (user guide);
- 9.1.4.3. Checklists operacionais e procedimentos padronizados (SOPs);
- 9.1.4.4. Slides e/ou apostilas utilizados durante o treinamento;
- 9.1.4.5. Gravação das sessões (quando realizadas de forma remota);
- 9.1.4.6. Scripts e comandos utilizados na instalação/configuração.

9.1.5. O material entregue deverá estar em formato digital, organizado por tópicos e atualizados conforme a versão da solução implantada.

9.1.6. A CONTRATADA deverá disponibilizar canal para esclarecimento de dúvidas e canal para abertura de chamados para suporte.

9.2. Treinamento Hands-on

9.2.1. O escopo do TREINAMENTO HANDS-ON refere-se ao funcionamento de treinamento prático da Solução ofertada, a ser ministrado pela CONTRATADA, abrangendo o pleno atendimento aos itens que seguem.

9.2.2. Fica sob responsabilidade da CONTRATADA ofertar treinamento/repasso de conhecimento sobre todas as funcionalidades da solução, com profissionais devidamente capacitados e aptos para exercer a função de instrutor.

9.2.3. A data de início do treinamento será estabelecida em comum acordo entre a CONTRATANTE e a CONTRATADA.

9.2.4. O treinamento deverá ser realizado de forma virtual, por meio de videoconferência, em língua portuguesa (Brasil), obrigatoriamente, utilizando ferramenta própria da CONTRATADA.

9.2.5. A carga horária do treinamento deverá ser de, no mínimo, 32 (trinta e duas) horas.

9.2.6. O treinamento deverá ser realizado com carga horária máxima diária de 04 (quatro) horas por turma, entre 08:00h e 17:00h, com intervalo mínimo de 15 (quinze) minutos.

9.2.7. O horário a ser executado será definido em comum acordo entre a CONTRATADA e a CONTRATANTE.

9.2.8. O programa do treinamento deverá abordar as principais funcionalidades de administração, configuração e operação da solução, sendo previamente aprovado pela CONTRATANTE. Eventuais mudanças de conteúdo solicitadas deverão constar no material didático.

9.2.9. O treinamento deverá abordar, minimamente, mas não se limitando, os conteúdos programáticos abaixo:

9.2.9.1. Visão geral da solução: arquitetura, componentes, recursos e funcionalidades;

9.2.9.2. Cenários de implantação;

9.2.9.3. Instalação e configurações iniciais dos componentes fundamentais da solução;

9.2.9.4. Instalação e configurações de clientes e/ou agentes;

9.2.9.5. Integração com outras soluções;

9.2.9.6. Cópias de segurança (backup) e restauração (restore) do ambiente;

9.2.9.7. Recursos e funcionalidades da interface administrativa;

9.2.9.8. Operação e administração da solução;

9.2.9.9. Gerenciamento de atualizações de software;

9.2.9.10. Estratégias de recuperação em caso de falha do servidor;

9.2.9.11. Monitoramento da solução, gerenciamento de eventos e incidentes;

9.2.10. O treinamento deverá desenvolver o conhecimento e as habilidades necessárias para o uso pleno de todos os recursos disponíveis na solução adquirida.

9.2.11. O material didático deverá ser disponibilizado em formato eletrônico, sem custo adicional para a CONTRATANTE, em língua portuguesa (Brasil).

9.2.12. Deverá ser emitido certificado de participação ao final do curso, contendo data, carga horária, conteúdo ministrado, nome completo do instrutor, nome completo do aluno, instituição responsável pelo treinamento e período de realização.

9.2.13. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE após a emissão da Ordem de Serviço, durante a primeira reunião de planejamento.

9.2.14. A CONTRATADA deverá realizar o treinamento HANDS-ON para a CONTRATANTE acerca das soluções implementadas ao longo da vigência do contrato, podendo ser realizados treinamentos individuais ou em turmas fechadas, conforme a necessidade da CONTRATANTE.

10. DA QUALIFICAÇÃO TÉCNICA

10.1. Da Comprovação de Atendimento Técnico e Capacidade Operacional

10.1.1. A empresa licitante deverá comprovar sua capacidade técnica e a aderência da solução ofertada às exigências estabelecidas nesta Especificação Técnica, assegurando que possui experiência, competência e recursos necessários para a implantação e suporte da solução de Gerenciamento de Acessos Privilegiados (PAM), na modalidade SaaS.

10.1.2. A comprovação da aderência técnica da solução deverá ser realizada por meio da apresentação de documentação oficial emitida pelo fabricante da solução ofertada, contendo descrições claras, objetivas e completas das funcionalidades exigidas, incluindo:

- Nome da solução, marca, versão e modelo ofertado;
- Lista de módulos e funcionalidades ofertadas;
- Arquitetura da solução (cloud-native/SaaS);
- Requisitos de integração com o ambiente do cliente;
- Funcionalidades específicas como: cofre de senhas, gravação de sessões, workflow de aprovação, integração com Active Directory, gestão de acessos remotos, auditoria e relatórios;
- Mecanismos de segurança e alta disponibilidade.

10.1.3. A documentação deverá vir acompanhada de uma tabela de referência cruzada, nos moldes abaixo, indicando com precisão onde está cada evidência técnica de atendimento aos requisitos:

Item da Especificação	Documento	Página	Localização
2.1.1	Manual da Solução PAM	4	Sexto parágrafo
3.2.4	Guia Técnico v3	25	Tabela 2
...	...	...	...

10.1.4. A ausência da tabela ou a apresentação de documentação incompleta, genérica ou sem correspondência direta com os requisitos técnicos poderá resultar na desclassificação da proposta.

10.1.5. A CONTRATANTE se reserva o direito de realizar diligências junto ao fornecedor da solução para confirmar a autenticidade e veracidade da documentação apresentada, bem como validar a existência dos módulos e funcionalidades exigidas.

10.1.6. Além da documentação da solução, a empresa licitante deverá apresentar atestado(s) de capacidade técnica, emitido(s) por órgão(s) da administração pública ou entidade(s) privadas, em papel timbrado e devidamente assinados, que comprovem já ter fornecido, implantado ou mantido solução de natureza similar ao objeto deste Termo de Referência, incluindo serviços de:

- Implantação de solução PAM em ambiente corporativo;
- Instalação e configuração de módulos técnicos;
- Integração com diretórios (AD, LDAP) e autenticação (MFA, RADIUS);
- Gestão de acessos remotos e gravação de sessões privilegiadas;
- Treinamento e repasse de conhecimento técnico à equipe do cliente.

- 10.1.7. Será permitida a apresentação de múltiplos atestados, desde que, somados, comprovem o atendimento integral às exigências deste item.
- 10.1.8. A análise da qualificação técnica será conduzida pela área técnica e/ou comissão de licitação do SENAC/ES, que poderá, a seu critério, solicitar esclarecimentos adicionais, documentação complementar ou realizar diligências para validação das informações apresentadas.
- 10.1.9. As exigências deste item visam garantir a seleção de fornecedores que demonstrem efetiva capacidade técnica para fornecer, implantar e manter a solução proposta, em conformidade com as normas de segurança da informação, boas práticas do setor e os requisitos regulatórios aplicáveis.

11. DO PAGAMENTO

11.1. DA FORMA DE PAGAMENTO E DAS CONDIÇÕES FINANCEIRAS

- 11.1.1. O pagamento será realizado de forma mensal, mediante apresentação de Nota Fiscal eletrônica (NF-e) devidamente atestada pelo setor competente da CONTRATANTE, no prazo máximo de 20 (vinte) dias corridos após a entrega da documentação fiscal.
- 11.1.2. A Nota Fiscal deverá estar acompanhada da seguinte documentação obrigatória e válida na data da emissão:
- Certidão Negativa de Débitos com a Receita Federal e Dívida Ativa da União (CND);
 - Certidões Negativas de Débitos Estaduais e Municipais do domicílio ou sede da empresa;
 - Comprovante de regularidade trabalhista, quando exigidos.
- 11.1.3. O pagamento estará condicionado à efetiva prestação dos serviços contratados e a disponibilização contínua da solução SaaS, conforme obrigações definidas na Especificação Técnica.
- 11.1.4. A CONTRATANTE poderá deduzir do valor a ser pago quaisquer multas, penalidades, glosas ou compensações previstas contratualmente.
- 11.1.5. Nenhum pagamento será efetuado caso a CONTRATADA esteja em situação irregular com obrigações fiscais, trabalhistas ou previdenciárias, ou ainda, caso esteja pendente de entrega de documentos obrigatórios ou da devida regularização de faturas anteriores com inconsistências.
- 11.1.6. Havendo erro na Nota Fiscal ou documentação, esta será devolvida à CONTRATADA para correção, ficando o prazo de pagamento suspenso e reiniciado a partir da data de reapresentação correta, sem ônus adicional para o SENAC/ES.

12. PROVA DE CONCEITO (POC)

12.1. Requisitos Gerais

- 12.1.1. Poderá ser exigida uma Prova de Conceito (POC) que tem como objetivo validar, de forma prática, a eficácia, desempenho, funcionalidades e aderência da solução de Privileged Access Management (PAM) ofertada, garantindo que atenda plenamente às necessidades técnicas, operacionais e de segurança da informação do SENAC ES.
- 12.1.2. A POC deverá ser realizada presencialmente ou remotamente no ambiente controlado da LICITANTE, devendo a CONTRATADA disponibilizar todos os recursos necessários, incluindo ambientes, licenças temporárias, infraestrutura de demonstração.
- 12.1.3. A POC deverá demonstrar, obrigatoriamente, a operação completa da solução de PAM, com foco em controle, proteção, auditoria, segregação de acesso privilegiado e funcionalidades avançadas.

12.1.4. A solução deverá demonstrar:

Serviço Nacional de Aprendizagem Comercial
Departamento Regional no Espírito Santo

Av. Marechal Mascarenhas de Moraes, 2077
Bento Ferreira - Vitória/ES - CEP 29050-935
Telefax: (27) 3325-8311 - www.es.senac.br

12.1.4.1. Cofre de Credenciais

- Armazenamento seguro de credenciais privilegiadas com criptografia forte (AES-256 ou superior);
- Rotação automática de senhas (Windows, Linux, banco de dados, dispositivos de rede);
- Políticas de complexidade e expiração configuráveis;
- Descoberta automática de contas privilegiadas no ambiente (AD, servidores etc.).

12.1.4.2. Sessões Privilegiadas

- Acesso a ativos sem exposição de senhas ao usuário;
- Gravação completa de sessões (RDP, SSH, Web, Banco de Dados);
- Reprodução da sessão gravada;
- Pesquisa por comandos executados (em sessões SSH);
- Encerramento forçado de sessão em tempo real.

12.1.4.3. Controle de Acesso

- Criação de perfis com segregação de função;
- Aprovação em múltiplos níveis (workflow);
- Acesso temporário (Just-in-Time - JIT);
- Expiração automática de privilégios.

12.1.4.4. Auditoria e Conformidade

- Trilha completa de auditoria;
- Relatórios exportáveis (PDF, CSV);
- Relatórios de:
 - ✓ Acessos privilegiados
 - ✓ Falhas de autenticação
 - ✓ Alterações de políticas

12.1.4.5. Segurança da Solução

- MFA nativo ou integração com MFA externo;
- Backup e recuperação da base do cofre;
- Hardening documentado.

12.2. Gestão e Cofre de Senhas

12.2.1. Demonstração da capacidade de armazenar, proteger e rotacionar automaticamente credenciais privilegiadas (senhas de administrador, contas de serviço, root etc.)

12.2.2. Exibição do cofre seguro, com validação de criptografia, controle de acesso e trilhas de auditoria.

12.3. Descoberta de Ativos e Contas Privilegiadas

12.3.1. Detecção de servidores, dispositivos de rede, serviços e contas privilegiadas.

12.3.2. Mapeamento automático de contas órfãs ou não gerenciadas.

12.4. Sessões Privilegiadas

12.4.1. Demonstração de acesso remoto seguro sem exposição de senhas (passwordless vaulting).

12.4.2. Capacidade de gravação de sessões em vídeo, incluindo busca textual dentro do conteúdo gravado.

12.4.3. Controles de autorização, incluindo workflow de aprovação para sessões críticas.

12.5. Just-in-Time Access (JIT)

- 12.5.1. Concessão temporária de privilégios, acesso sob demanda e elevação de privilégios granular.
- 12.5.2. Expiração automática dos acessos e auditoria detalhada.

12.6. Controle de Comandos e Auditoria Avançada

- 12.6.1. Restrição, bloqueio ou revisão de comandos executados durante sessões privilegiadas.
- 12.6.2. Geração de trilhas de auditoria completas: usuário, dispositivo, horário, comandos e ações críticas.
- 12.6.3. Integração com MFA (Multi-Fator de Autenticação).
- 12.6.4. Integração com SIEM/SOC para envio de logs, eventos e alertas.

12.7. Políticas e Fluxos de Acesso

- 12.7.1. Criação e demonstração de políticas de controle de acesso privilegiado para servidores, aplicações e dispositivos de rede.
- 12.7.2. Configuração de fluxos de aprovação para ações sensíveis.

12.8. Segurança, Monitoramento e Alertas

- 12.8.1. Demonstração de alertas para atividades suspeitas, uso anômalo de privilégios ou tentativas de acesso não autorizado.
- 12.8.2. Painel gerencial com visão consolidada de riscos, contas, sessões e incidentes.

12.9. Relatórios e Compliance

- 12.9.1. Geração de relatórios nativos da solução para auditorias, incluindo:
 - 12.9.1.1. Relatórios de acesso, sessões, comandos e alterações;
 - 12.9.1.2. Relatórios de senhas rotacionadas e políticas aplicadas.

12.10. Caso Prático de Uso Real

- 12.10.1. Acesso de um administrador a um servidor Windows e Linux;
- 12.10.2. Execução de tarefa administrativa com trilha de auditoria completa;
- 12.10.3. Abertura e encerramento de sessão privilegiada;
- 12.10.4. Rotação automática da senha após a sessão.

12.11. Relatório Final

- 12.11.1. Descrição detalhada dos cenários demonstrados;
- 12.11.2. Funcionalidades atendidas e não atendidas;
- 12.11.3. Evidências (prints, vídeos, logs);
- 12.11.4. Avaliação técnica da solução;
- 12.11.5. Checklist de conformidade com os itens exigidos no edital.