TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra, 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

ESTUDO TÉCNICO PRELIMINAR (DEMANDAS DE TIC) Nº STIC 05/2022 - TRE-ES/PRE/DG/STI/CIS/SRCD

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1 - CARACTERIZAÇÃO DA DEMANDA

1.1 - Descrição Sucinta

Aquisição de uma solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos), com capacidade para armazenar, proteger, controlar, gerenciar, auditar e monitorar o acesso privilegiado incluindo serviço de instalação e transferência de conhecimento.

1.2 - Justificativa da necessidade e Resultados

A aquisição da solução em questão visa proteger, controlar, gerenciar, auditar e monitorar contas privilegiadas a ativos críticos do TRE-ES. São considerados ativos críticos: equipamentos servidores físicos e virtuais que hospedam todos os

sistemas eleitorais, administrativos e judiciais; Servidores de Banco de Dados; Servidores de Arquivos Corporativos; Servidores de Correio Eletrônico, Equipamentos Firewalls, Controladoras, Switches de Rede, Contas de Serviços, dentre outros.

Por que proteger o acesso privilegiado?
As credenciais privilegiadas são os principais alvos de invasão dos cybercriminosos. Uma conta privilegiada comprometida pode, por exemplo, conceder acesso irrestrito à infraestrutura de TI da Companhia, possibilitando ao atacante ter o controle administrativo das demais contas, obter dados internos sensíveis. Toda esta facilidade de acesso, fará com que os danos sejam irreparáveis para a empresa afetada.
Desta forma, busca-se uma solução que garanta a segurança operacional por meio de trilha de auditoria dos indivíduos que têm acesso a dados sensíveis ou processos críticos de TI.

Entre os fatores que influenciam os ataques cibernéticos, o furto de informações pessoais e o roubo de identidades está no topo da lista. De acordo com o relatório do Breach Level Index, desde 2016 este é considerado o principal tipo de violação de dados, com 59% do total das ocorrências do ano.
Desse modo, a contratação tem como objetivos evitar os seguintes problemas:
- Acesso de várias pessoas utilizando a mesma conta. Desta forma é impossível manter a trilha de auditoria, pois existem vários logins ao mesmo tempo. Há, também, a responsabilidade (accountability) mínima do uso da conta, e, como é compartilhada, muitas vezes as pessoas não se sentem responsáveis pela segurança e fazem coisas que não fariam com o seu próprio usuário, como escrever a senha em algum post-it.
- Falta de gestão da senha: Imagine mudar uma senha compartilhada por muitos. Isso requer que a senha seja distribuída de uma maneira segura. Isto pode significar mais trabalho, e propensão a erros, além possíveis falhas no tratamento destes.
- Vazamento de senhas de contas de usuários com privilégios de administrador;
- Ataques hackers: uma vez que tendo acesso a contas privilegiadas podem assumir o controle total de um sistema, roubando informações, alterando configurações, indisponibilizando serviços ou até mesmo destruindo de forma permanente informações importantes.

2 - ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

2.1 - Requisitos Relacionados ao Negócio

A solução deve:

- Registrar os eventos realizados nas sessões privilegiadas;
- Prover de forma segura o armazenamento centralizado das credenciais e acesso dos ativos de rede em alta disponibilidade;
- Suportar integração com os sistemas internos do TRE;
- Registrar as ações realizadas em posse de conta privilegiada com possibilidade de gravação de sessão (gravação de telas);
- Melhorar controle sobre a utilização de recursos privilegiados do ambiente computacional;
- Obter o monitoramento das ações de servidores e terceirizados com o uso de credenciais privilegiadas;
- Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;
- Rastrear o uso de contas privilegiadas no ambiente computacional;
- Aprimorar a segurança da informação e comunicação do TRE;
- Permitir a exportação das credenciais e senhas em formato seguro.

2.2 - Requisitos de Capacitação, Ambientais, Culturais e Sociais

A contratação deve possuir um item transferência de conhecimento para capacitar os servidores da STI a operacionalizar a ferramenta.

2.3 - Requisitos de Manutenção

Não há requisitos de manutenção dos itens adquiridos, exceto quando houver mudança de versão do sistema operacional.

2.4 - Requisitos Temporais

As licenças adquiridas devem ser vitalícias (perpétuas) não havendo necessidade de renovação ao longo do tempo;

A garantia de atualização do software deve ser de, no mínimo, 60 (sessenta) meses;

2.5 - Requisitos de Segurança

A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.501/2016), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Espírito Santo aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

O Tribunal Regional Eleitoral da Espírito Santo terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS

3.1 - Características Gerais

3.1.1 - Auditoria e gerenciamento de acesso lógico por meio de credenciais privilegiadas para os dispositivos (ativos de rede e servidores físicos e virtuais de serviços e sistemas tecnológicos) do TRE-ES;

3.1.2 - As solução instalada no TRE-ES devem funcionar de maneira completamente independente;

3.1.3 - Para soluções que são licenciadas por usuários e não por dispositivos, deverá ser utilizado um fator de conversão de 10 usuários para cada 100 dispositivos. Caso o número de usuários resultante seja fracionado, este deverá ser arredondado para cima;

3.1.4 - . 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;

3.1.5. A solução deve mitigar problemas de segurança relacionados ao compartilhamento de contas que são armazenadas localmente em dispositivos e também para as contas que não são gerenciadas de forma centralizada por serviços de diretórios;

3.1.6. A solução deve descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados incluindo tarefas agendadas do Windows (Scheduled tasks) e Serviços Windows. Além disso, a solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas;

3.1.7. A solução deve garantir a quantidade de acessos a sua interface conforme a necessidade do Contratante e não deve limitar o número de contas que podem ser gerenciadas em um alvo licenciado;

3.1.8. A solução deve suportar métodos de alta disponibilidade para todos os componentes que fazem parte da solução, a fim de mitigar riscos inerentes à indisponibilidade destes. A solução deve ainda contemplar a expansão, incremento ou melhoria exclusivamente destes métodos sem qualquer custo adicional de licenciamento da solução para o Contratante;

3.1.9. A solução deve atender o conceito de tolerância a falhas e não ter restrições para funcionar em modo de alta disponibilidade ativo – ativo ou ativo – passivo;

3.1.10. A solução deve suportar alta disponibilidade ativo/passivo onde na falha do primário, o appliance ou servidor secundário deve assumir suas funções automaticamente permitindo a continuidade do acesso as contas privilegiadas;

3.1.11. O chaveamento do appliance/servidor primário para o appliance/servidor secundário deve ser feito por completo, incluindo funções primordiais como troca de senhas, gravação de sessões e etc;

3.1.12. Todas os controles de alta disponibilidade devem ser feitos via interface gráfica, sem depender de comandos manuais, scripts ou adaptações;

3.1.13. A sincronização de dados os servidores/appliances da solução deve ser gerenciada nativamente pela solução sem necessidade de intervenção manual para garantia de sincronia entre os dois appliances;

3.1.14. A solução deve utilizar um banco de dados não proprietário. O banco de dados deve permitir alta disponibilidade e mecanismos para a recuperação de desastres;

3.1.15. A ferramenta deverá permitir o backup e recovery de seu banco de dados, bem como das configurações de software estabelecidas, com as seguintes capacidades:

- Deverá permitir a execução de backups sem paradas do sistema;

- Deverá permitir a execução de backups automatizados, permitindo a sua programação/agendamento;

3.1.16. A solução não deve utilizar qualquer tipo de agente, sejam eles nas consoles de gerenciamentos, dispositivos alvos ou em qualquer outro componente que faça parte da solução;

3.1.17. A solução deverá ser entregue em formato de appliance virtual para execução em máquinas físicas ou virtuais, virtualizadas sob a plataforma VMware, na versão 7.0;

3.1.18. Serão aceitas soluções entregues em software, desde que todos os componentes necessários para seu funcionamento (como sistema operacional, banco de dados e licenças adicionais necessárias) sejam contemplados na proposta e entrega da solução;

3.1.19. A solução deve possuir um dashboard ou método similar, que possa demonstrar a saúde da solução através de dados como utilização de disco, CPU, memória, serviços em execução, serviços parados e gráficos que demonstrem o uso de CPU;

3.1.20. A solução deve suportar a geração notificações por e-mail e/ou SNMP no caso em que os serviços essenciais sejam parados e/ou se problemas no hardware forem detectados;

3.1.21. A solução deve possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as senhas das credenciais gerenciadas pela mesma. Deve ainda ser compatível com os seguintes métodos de criptografia:

- AES com chaves de 256 bits;

- FIPS 140-2;

3.1.22. Suportar utilização de hardwares de HSM através de PKCS#11 ou superior;

3.1.23. 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;

3.1.24. A solução deverá ser capaz de exportar a chave de criptografia do local de armazenamento das credenciais (cofre), para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas gerenciadas pela solução;

3.1.25. A solução não deverá permitir a abertura do cofre com chaves criptográficas geradas por seus respectivos fornecedores e/ou fabricantes em hipótese alguma;

3.1.26. A solução deve suportar integrar-se com soluções de autenticação de duplo fator através de protocolo Radius ou SAML;

3.1.27. A solução deve disponibilizar a opção de autenticação utilizando certificados (Smart Cards) e protocolo SAML 2.0;

3.1.28. A solução deve prover uma interface gráfica para que os administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros;

3.1.29. A solução deve integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas, das seguintes ações:
- Atividades administrativas relacionada a acesso as credenciais privilegiadas;

- Atividades de recuperação, liberação e alterações de senhas;

- Outras atividades de executadas pelos usuários na console web.

3.1.30. A solução deve suportar, sem necessidade de licenciamento adicional, a gestão de senhas no código fonte em aplicações e scripts (AAPM) através de uma API REST;

3.1.31. A solução deve possuir API REST, onde as aplicações consomem a senha com requisições à interface API REST, assim evitando que as senhas fiquem expostas no código fonte das aplicações;

3.1.32. A solução deve possuir mecanismo de cache para suportar milhares de requisições pelas aplicações simultaneamente;

3.1.33. A solução deve possuir mecanismo de segurança que libera o acesso a REST API somente a aplicativos autorizados, incluindo, no mínimo, filtro de IP de origem e autenticação por certificados;

3.1.34. A solução deve descobrir e alterar credenciais Windows, incluindo contas nomeadas, administradores 'built-in' e convidados;

3.1.35. A solução deve gerenciar credenciais de Banco de Dados, incluindo Microsoft SQL Server, PostgreSQL, Oracle, MongoDB e MySQL.

3.1.36. A solução deve descobrir e alterar credenciais privilegiadas em ambientes Linux;

3.1.37. Gerenciar credenciais em interfaces de gerenciamento de servidores "out-of-band", suportando, no mínimo, Dell iDRAC e HP iLO;

3.1.38. A solução deve descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP, sem necessidade de adaptações ou scripts;

3.1.39. O Sistema deve ser capaz de realizar a descoberta, armazenamento e gestão de chaves SSH em sistemas Linux;

3.1.40. A solução deve identificar as contas privilegiadas com ID 0 em Linux e as contas que não possuem ID zero, porém, são privilegiadas através do uso de ´sudo´ (configuradas no Sudoers);

3.1.41. A solução deve 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;

3.1.42. Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e deve ser capaz de realizar 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. 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;

3.1.43. 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:

- 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. Não deverá ser necessária interatividade por parte do usuário no processo de login ao sistema operacional do servidor de destino. Deverá ser possível habilitar a gravação da sessão caso seja necessário;

- Sistemas baseados em Remote Desktop e SSH sem que os usuários vejam a senha. A senha vigente no momento (estática ou dinâmica) deverá ser provida para as aplicações ou conexões remotas devendo ser recuperadas de forma automática e transparente do banco de dados da solução;

3.1.44. As sessões acessadas podem ser monitoradas por meio de gravação de vídeos das mesmas, em formato padrão de execução da solução;

3.1.45. A solução deve permitir que um administrador possa bloquear, desbloquear e terminar uma sessão ativa caso julgue necessário;

3.1.46. Monitorar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado;

3.1.47. A solução deve possuir a opção de terminar a sessão automaticamente em uma sessão SSH se o usuário digitar um comando não autorizado;

3.1.48. A solução deve permitir que as sessões SSH e RDP abertas através da solução sejam terminadas de forma automática ao expirar o tempo requisitado de sessão;

3.1.49. A solução deve permitir que seja forçado o logoff do usuário em sessões RDP terminadas pela solução ao final do tempo de requisição da sessão;

3.1.50. A solução deve permitir que os usuários solicitem acesso aos gestores através de interface Web, preferencialmente, em HTML5;

3.1.51. A solução deve fornecer uma aplicação Web para acessar as funcionalidades básicas que seja compatível, no mínimo, com Internet Explorer, Google Chrome e Firefox;

3.1.52. Oferecer em sua aplicação web diferentes visões de acordo com as permissões dos usuários mostrando, por exemplo, apenas os ativos e contas delegadas àquele usuário;

3.1.53. A solução deve permitir o envio automático de logs para servidores SYSLOG de forma aderente ao disposto em RFC 5424 - The Syslog Protocol (IETF);

3.1.54. A solução deve registrar cada acesso incluindo, no mínimo, os acessos via aplicação web para solicitações de senha, aprovações, retirada de senhas, mudanças de delegação e relatórios. Devem ser registrados os acessos à Console de Gerenciamento tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas;

3.1.55. Criar relatórios que podem ser exportados em formatos editáveis suportando, no mínimo, os formatos HTML e derivados, CSV, XLSX ou XLS;

3.1.56. A solução deve suportar também a criação de relatórios que podem ser exportados em formatos não editáveis suportando, no mínimo, o formato PDF;

3.1.57. O gerenciamento de identidades privilegiadas deverá disponibilizar:

- Mecanismo de retirada e devolução de contas e senhas compartilhadas;

- Definição de tempo de validade: permitir o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;

- Troca automática da senha no sistema gerenciado, após a sua devolução;

- Troca automática da senha no sistema gerenciado, após o vencimento do tempo de validade estabelecido;

- Configuração de calendário de requisição de senhas de identidades privilegiadas com base em usuários ou grupos de usuários;

- Troca de Senhas por Demanda: Permitir a troca de senhas nos Sistemas Gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (Grupo de Todos os Sistemas Operacionais , por exemplo);

3.1.58. Dessa forma, no processo de definição da política de composição de senha, a solução deve ser capaz de:

- Gerar senhas aleatórias com extensão de 128 (cento e vinte e oito) caracteres ou mais;

- Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos;

- Especificar qual o tipo de caractere na composição das senhas a serem geradas;

- Suportar controle de acesso baseado em papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada. Deve permitir a formação de grupos de usuários e dispositivos, bem como a atribuição de privilégios de

acesso a esses Grupos, onde esses privilégios de acessos possam ser atribuídos por critérios como tipo de dispositivo: sistemas operacionais, banco de dados;

- Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha;

- Garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial;

- Garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo;

3.1.59. Permitir a definição de fluxos de aprovação (workflows) para obtenção de acesso às contas privilegiadas, com as seguintes características:

- Personalização de fluxos: Permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta (como de acesso emergencial, de uso por terceiros), e aprovação de pelo menos um responsável;

- 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;

- A solução deve ser capaz, caso seja necessário, de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço ou tarefas agendadas do Windows em todos os locais onde estejam sendo utilizadas;

- Caso seja necessário, após alteração da senha de identidade privilegiada associada à um serviço, a solução deverá ser capaz de reinicializar o mesmo;

- A descoberta automática deve ser realizada por buscas no Active Directory (AD) e/ou por ranges de endereços IP;

3.1.60. Sobre as características da interface Web para acesso de recuperação das senhas, a solução deverá ser capaz de:

- Suportar de forma nativa a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução;

- Permitir que as páginas Web sejam personalizadas de acordo as preferências de linguagem individuais do usuário, inclusive com o idioma em Português;

3.1.61. A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como:

- Lista de sistemas gerenciados;

- Senhas armazenadas;

- Eventos de alteração de senha;

- Auditoria de contas;

- Auditoria de sistemas;

- Auditoria de usuários;

- Detalhes das próximas atualizações de senha programadas;

- Sistemas que estão usando uma conta de serviço para iniciar um ou mais serviços.

3.1.62. A solução deve fornecer relatórios de auditoria que disponibilizem detalhes das interações dos usuários com a solução, tais como:

- Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários;

- Alterações nas funções de delegação;

- Adições, deleções, alterações de senhas gerenciadas pela solução;

- Operações das senhas dos usuários, incluindo check-in e checkout, solicitações negadas e permitidas;

- Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e assim por diante;

3.1.63. O Sistema deve possuir função de monitoramento e análise de comportamento que toma por base os eventos gerados por todos os itens desta especificação técnica;

3.1.64. Através dos eventos coletados, deve montar perfis de comportamento dos usuários do sistema;

3.1.65. A solução deve alertar abusos e comportamentos fora dos padrões aprendidos/mapeados;

3.1.66. A solução deve monitorar e exibir acessos e atividades realizadas no próprio sistema;

3.1.67. A solução deverá exibir o somatório das atividades diárias divididos por origem;

3.1.68. A solução deve detectar, pelo menos, os seguintes comportamentos anormais:

- Acessos excessivos a contas privilegiadas;

- Usuários potencialmente não confiáveis utilizando acessos administrativos ou contas locais;

- Primeira liberação de senha para uma conta gerenciada em um sistema;

- Usuários não conseguem recuperar a senha para uma solicitação aprovada ou se a senha é recuperada mais de uma vez;

3.1.69. Deve fornecer meio de integração para que soluções de terceiros possam encerrar sessões suspeitas (ex: SIEM executa terminação de sessão) através de integração via API;

3.1.70. Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em comandos Linux em sessões SSH, com suporte a expressões regulares para comandos em geral;

3.1.71. Módulo de Acesso Remoto Seguro:

3.1.71.1. O Módulo de acesso remoto seguro de executar em appliance virtual on-premises suportando, no mínimo, VMWARE 7.0;

3.1.71.2. O Módulo de acesso remoto seguro deve suportar o acesso externo a rede, sem necessidade de uma VPN;

3.1.71.3. A solução deve ser implantada localmente, com modelo de alta disponibilidade, continuidade de negócios e formas de recuperação de desastre;

3.1.71.4. A solução deve permitir o acesso a vários tipos de Sistemas Operacionais, com ou sem agentes, incluindo, no mínimo, o suporte a estações de trabalho Windows 10, Servidores Windows Server 2012, 2016 e 2019 e Linux RedHat Enterprise 6.x, 7.x e 8.x;

3.1.71.5. A solução não deve utilizar protocolos de comunicação legados necessários para o acesso, fazendo uso de TLS 1.2 ou superior;

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

3.1.71.7. A solução deve suportar o acesso desacompanhado, sem necessidade de permissão prévia a desktops e servidores;

3.1.71.8. A solução deve possibilitar o acesso a dispositivos de rede como roteadores, switches e outros dispositivos via SSH. Este acesso deve ser feito de forma local, sem que haja a necessidade de trafegar estes protocolos em redes inseguras e/ou liberando-os em regras de firewall;

3.1.71.9. A solução deve disponibilizar ao usuário, no mínimo, as seguintes formas de acesso a console da solução:

- Console instalada na estação do usuário, suportando os sistemas operacionais Windows em 32 e 64 Bit, MacOs e Linux em 32 ou 64Bit;

- Console de acesso Web, preferencialmente em HTML5, sem necessidade de nenhum plug-in ou agente especial para fornecer o acesso;

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

3.1.71.11. Suportar integração com soluções de autenticação de dois fatores via RADIUS ou SAML;

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

3.1.71.13. A solução deve suportar o uso de um certificado válido assinado por uma CA;

3.1.71.14. A solução deve possuir políticas para controlar quando os ativos podem ser acessados suportando, no mínimo:

- Programação para definir quando os ativos sob esta política podem ser acessados. A política deve permitir a definição do fuso horário a ser utilizado no agendamento, permitindo uma ou mais opções de agendamento do acesso. Definindo o dia e hora de início e o dia e hora de término;

- Para certos grupos de usuários, a solução deve permitir forçar o encerramento da sessão. Forçando a sessão a se desconectar no horário final agendado. Nesse caso, o usuário deve receber notificações antes de ser desconectado;

- Notificar destinatários quando uma sessão é iniciada. Suportando, no mínimo, uma notificação por e-mail a destinatários designados sempre que uma sessão é iniciada com qualquer ativo;

- Notificar destinatários quando uma sessão é terminada. Suportando, no mínimo, uma notificação por email a destinatários designados sempre que uma sessão é encerrada com qualquer ativo;

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

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

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

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

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

3.1.71.20. A solução deve suportar filtro de comandos durante as sessões SSH, visando evitar que o usuário, inadvertidamente, use um comando que pode causar danos ao servidor acessado;

3.1.71.21. A solução deve suportar a injeção automática de credenciais, permitindo que os usuários autentiquem ou elevem privilégios para desktops e sistemas remotos, sem revelar credenciais e senhas de texto simples. Deverá ser permitido ao usuário selecionar a credencial a ser utilizada a partir de uma lista de credenciais que têm privilégios nos sistemas aprovados para acesso;

3.1.71.22. A injeção de senhas deve suportar a integração com a solução de gerenciamento de acessos privilegiados, permitindo que seus usuários usem as senhas armazenadas na solução;

3.1.71.23. Ao acessar um ativo baseado em Windows, a injeção de credenciais deve ser suportada na tela de login, bem como a ação especial "Executar como";

3.1.71.24. Ao acessar um ativo baseado em Linux, injeção de credenciais deve suportar sua utilização em conjunto com o SUDO;

3.1.71.25. A solução deve suportar o acesso a desktops, servidores e outros sistemas remotos autônomos, suportando os seguintes modos:

- Através de clientes instalados, que permite o acesso a qualquer sistema Windows, Mac ou Linux. Tendo total gerência e relatórios centralizados de todos os clientes implantados;

- Acesso através de cliente de proxy local, que permite o acesso a sistemas Windows autônomos em uma rede, sem cliente pré-instalado;

- Acesso via cliente de proxy para acessar sistemas em uma rede remota que não tenha uma conexão de internet nativa;

3.1.71.26. Integração com RDP (Remote Desktop Protocol) da Microsoft para realizar sessões utilizando protocolo RDP. Permitindo que os usuários colaborem em sessões e estas sessões possam ser auditadas e gravadas automaticamente;

3.1.71.27. Acesso a dispositivos de rede habilitados para SSH através de um cliente de proxy efetuando a conexão localmente;

3.1.71.28. Acesso a servidores VNC onde os usuários podem colaborar em sessões e ter as sessões auditadas e gravadas automaticamente;

3.1.71.29. Acesso a páginas Web a partir de agente de proxy local, onde os usuários receberão apenas uma conexão a uma página Web local em uma sessão auditada e gravada;

3.1.71.30. Túnel de protocolos que permitem estender os recursos de conectividade e auditoria remotas de aplicativos proprietários e/ou de terceiros, como sistemas de controle de integração ou ferramentas de banco de dados personalizadas sem necessidade de VPN;

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

3.1.71.32. A solução deve permitir que os administradores possam encerrar as sessões em andamento, se necessário;

3.1.71.33. A solução deve permitir configuração de tempos limites de sessão ociosos, onde seja possível definir o tempo máximo para que um usuário inativo seja desconectado automaticamente;

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

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

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

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

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

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

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

3.1.71.41. A solução deve permitir que os usuários reiniciem um sistema durante a sessão e reconectem-se automaticamente quando ativo estiver on-line novamente;

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

3.1.71.43. A solução deve permitir o uso de credenciais armazenadas na solução de gerenciamento de acesso privilegiado para executar ações especiais, permitindo a execução de aplicativos (função de "executar como");

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

3.1.71.45. Solução deve possuir relatórios das sessões de acesso, onde seja possível visualizar todas as sessões, e detalhes destas sessões que incluem informações básicas da sessão, detalhes da sessão,

transcrições de bate-papo e gravações em vídeo de compartilhamento de tela, shells de comando e utilização de túnel de protocolos;

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

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

3.1.71.48. A solução deve apresentar em relatório as sessões que possuem a gravação ativada, uma opção para reprodução de vídeo de sessões individuais, incluindo legendas de quem estava no controle do mouse e do teclado em qualquer ponto determinado durante a sessão;

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

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

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

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

3.2 - Serviço de Instalação, Configuração e Transferência de Conhecimento

3.2.1. A Contratada será inteiramente responsável pela instalação da solução, bem como pelas despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

3.2.2. A instalação da solução deverá ser realizada remotamente, no ambiente do TRE-ES;

3.2.3. A instalação da solução deverá ser realizada em dias úteis, podendo ocorrer no período de 10h às 19hs, considerando o fuso horário do contratante;

3.2.4. O processo de instalação da solução deverá ser acompanhado por servidores do Contratante;

3.2.5. Para garantir que a instalação não afetará o ambiente do Contratante, os procedimentos e atividades deverão ser realizados por técnicos certificados na solução;

3.2.6. A Contratada deverá se reunir com a equipe técnica do Contratante e elaborar um plano de instalação, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço;

3.2.7. A contratada deverá realizar a instalação de todos os módulos adquiridos, bem como realizar a configuração do gerenciamento de acesso privilegiado em 10 (dez) dispositivos, sendo eles 3 (três) servidores linux, 2 (dois) servidores de domínio Windows, 1 (um) VMWARE Vcenter, 2 (dois) Hosts ESXi e 2 (dois) equipamentos de firewall;

3.2.8. A instalação da solução no ambiente do Contratante não poderá interferir no bom funcionamento de outros sistemas previamente instalados;

3.2.9. A transferência de conhecimento deverá ser realizada no próximo dia útil após a conclusão do serviço de instalação e configuração da solução;

3.2.10. O repasse de conhecimento deverá ter duração mínima de 20 (vinte) horas;

3.2.11. A Contratada deverá realizar a transferência de conhecimento para a equipe técnica do Contratante, por meio de repasse de conhecimento nas tecnologias da solução;

3.2.12. A transferência de conhecimento deverá ser realizada de forma remota, por meio de ferramenta a ser acordada com o Contratante;

3.2.13. A transferência de conhecimento deverá conter conteúdo teórico e prático sobre a solução e deverá abordar, no mínimo, os seguintes itens:

- Detalhamento dos componentes da solução, suas interconexões e todas as informações técnicas necessárias para o seu pleno funcionamento;

- Orientar sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes da solução, informando as interconexões realizadas com a infraestrutura existente no Contratante;

- Orientar sobre os componentes, procedimentos de instalação e administração da solução, explorando as funcionalidades disponíveis na solução ofertada, ainda que não exigidas na especificação técnica;

3.2.14. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelo fabricante dos softwares da solução ofertada;

3.2.15. Concluir instalação, configuração e transferência de conhecimento da solução no prazo de 30 (trinta) corridos, contados do recebimento provisório;

3.2.16. Caso seja de comum acordo entre o Contratante e a Contratada, as atividades remotas relacionadas no item 3.2 e subitens poderão ser realizadas presencialmente.

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

A única solução que atende todos os requisitos tecnológicos e a aquisição de sistema cofre de senhas.

4.1. Cofre de Senhas

Descrição da solução: Sistema que permita a gestão das credenciais privilegiadas, rotacionamento de senhas periodicamente com controle de acesso a cada credencial.

Órgão /Entidade Proprietário da Solução: Não se aplica à presente contratação.

Aderência da Solução ao MNI: Não se aplica à presente contratação.

Aderência da Solução ao ICP-Brasil: Não se aplica à presente contratação.

Aderência da Solução ao Moreq-Jus: Não se aplica à presente contratação.

5 - INDICAÇÃO DA STIC ESCOLHIDA

5.1 - Descrição da Solução

Nome: Cofre de Senhas

Descrição: Aquisição de software de Cofre de Senhas para gestão de acessos privilegiados, rotacionamento periódico de senhas e controle o acesso a cada credencial, com suporte e garantia de versionamento por 60 meses.

Valor Estimado: R$ 572.500,00 (Quinhentos e setenta e dois mil e quinhentos reais).

5.2 - Justificativa/Motivação da Escolha

A solução de cofre de senhas é a única que atende a todos os requisitos exigidos;

5.3 - Aderência aos Requisitos

Os requisitos tecnológicos estão aderentes aos requisitos funcionais estabelecidos pelo demandante.

5.4 - Relação entre a Demanda Prevista e a STIC

O TRE-ES possui aproximadamente 350 (trezentos e cinquenta) dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos) que possuem acesso privilegiados para os quais é necessário um gerenciamento de credencias, de acordo com a tabela abaixo:

ITEM	QUANTIDADE
Dispositivos de rede	50
Servidores: hipervisor VMWARE, VMs, Windows e Linux	180
Instâncias de banco de dados Oracle e Postgres	20
Instâncias de aplicações/serviços corporativos/senhas hardcode	100
TOTAL	**350**

Assim o TRE-ES necessitará de 350 licenças do software de cofre de senhas para permitir a gestão de credenciais privilegiadas nestes dispositivo.

Em consonância com o que está disposto no Termo de Referência do TSE (0684549) será necessário adquirir:

Item 1 - Solução de Gerenciamento de Acessos Privilegiados, com garantia técnica de 60 (sessenta) meses: 350 licenças.

Item 2 - Serviço de Instalação, Configuração e Transferência de Conhecimento: 1 .

ITEM	DESCRIÇÃO	QUANTIDADE
1	Solução de Gerenciamento de Acessos Privilegiados, com garantia técnica de 60 (sessenta) meses	350
2	Serviço de Instalação, Configuração e Transferência de Conhecimento	1

6 - INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

Não existem necessidades de adequação ambiental.

ANÁLISE DE RISCOS

7 - IDENTIFICAÇÃO DOS RISCOS

O principal risco identificado foi:

- Não cumprimento do prazo de entrega pela contratada.

8 - RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

RISCO 1	NÃO CUMPRIMENTO DO PRAZO DE ENTREGA PELA CONTRATADA	
Probabilidade: (Alta, média ou baixa)	**Baixa**	
	Efeito (Dano)	**Impacto:** (Alto, médio ou baixo)
1	Atraso na implementação do gerenciamento de senhas	Baixo
	Ações de Mitigação e Contingência	**Responsável**
1	Acompanhar rigorosamente o processo de contratação	Integrante Demandante

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

9. RECURSOS MATERIAIS E HUMANOS

Trata-se de aquisição de licenciamento de software. A instalação e configuração inicial serão realizadas pela contratada. A contratada também será responsável pelo repasse de conhecimento para operação da solução com período mínimo de 20 horas.

10. DESCONTINUIDADE DO FORNECIMENTO

Não se aplica. Compra de licenciamento de software em parcela única.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Demandante: Rommel Baia Silva (substituto: Lucas Ribeiro Carlin)

Integrante Técnico: Lucas Ribeiro Carlin (substituto: Rommel Baia Silva)

Integrante Administrativo: Marcos Venturott Ferreira (substituto: Carlos Alberto da Rocha Pádua Filho)

Vitória, 03 de março de 2022.

Documento assinado eletronicamente por **MARCOS VENTUROTT FERREIRA**, **Integrante Administrativo**, em 03/03/2022, às 18:18, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUCAS RIBEIRO CARLIN**, **Técnico Judiciário**, em 03/03/2022, às 18:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ROMMEL BAIA SILVA**, **Chefe de Seção**, em 03/03/2022, às 18:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0699555** e o código CRC **B12326CA**.

0000662-23.2022.6.08.8000 0699555v3