REQUEST FOR PROPOSAL – RFP

SOLUÇÃO DE GERENCIAMENTO DE ACESSOS PRIVILEGIADOS, ALÉM DOS SERVIÇOS DE PLANEJAMENTO, IMPLANTAÇÃO, MIGRAÇÃO, TREINAMENTO, SUPORTE, ASSISTÊNCIA TÉCNICA E CONSULTORIA

ANEXO II
REQUISITOS DA SOLUÇÃO

1. REQUISITOS GERAIS DA SOLUÇÃO

1.1. Os REQUISITOS GERAIS DA SOLUÇÃO aplicam-se à Solução considerada em sua totalidade.
1.2. Os requisitos constantes deste documento têm caráter obrigatório devendo ser rigorosamente atendidos pelos fornecedores sob pena de desclassificação da proposta e sujeição à aplicação de sanções contratuais.
1.3. Todos os componentes de *software* da Solução deverão constar do catálogo do mesmo fabricante e seus parceiros de tecnologia homologados. Não serão aceitas composições *ad hoc* elaboradas com o objetivo de atender às especificações deste certame.
1.4. No momento da apresentação das propostas, todos os componentes de software constantes da Solução deverão possuir EOL (*End-of-life*) e EOS (*End-of-support*) não definidos ou anunciados para um prazo superior a 36 (trinta e seis) meses.
1.5. O modelo de licenciamento dos *softwares* que compõem a Solução deverá contemplar a modalidade de subscrição para o Banco.
1.6. Todos os componentes da Solução deverão ser fornecidos com a versão mais atualizada dos *softwares* e *firmwares* considerando-se a data da implantação.
1.7. Serão 2 (dois) os locais de implantação da Solução a ser adquirida por meio desta licitação, a saber: sítio primário e sítio secundário, sendo ambos situados no campus do CAPGV (Centro Administrativo Presidente Getúlio Vargas) localizado em Fortaleza-CE. O Banco reserva-se o direito de alterar, até a fase de implantação da Solução, o local de implantação do sítio secundário, ficando o novo local restrito a área geográfica da RMF (Região Metropolitana de Fortaleza) sem que isso incorra em qualquer tipo de ônus para o Banco.
1.8. A Solução terá todos os seus recursos e capacidades implantados em ambos os sítios, de maneira igualmente dividida para acesso simultâneo.
1.9. Todos os componentes da Solução deverão ser fornecidos para o ambiente de homologação.
1.10. Todos os componentes de *software* da Solução deverão guardar total compatibilidade entre si, não podendo o licitante alegar eventuais incompatibilidades de qualquer ordem para deixar de cumprir os requisitos desta RFP.
1.11. A Solução deve armazenar, de forma criptografada, e controlar as credenciais de acesso privilegiado constantes dos Dispositivos Gerenciados pela Solução.
1.12. Prover autenticação transparente no sistema-alvo ou dispositivo. A solução deve iniciar uma sessão injetando diretamente as credenciais na tela de login e servindo como um proxy para a sessão entre o usuário e o sistema-alvo, de forma que a senha não seja exposta ao solicitante do acesso.
1.13. Eliminar credenciais privilegiadas inseridas em códigos-fonte, scripts e arquivos de configuração, fazendo com que as senhas passem a ser gerenciadas pela solução e inacessíveis às equipes de suporte e desenvolvimento de TI, possuindo ainda, plugin/solução para navegador e prover o acesso remoto seguro ao ambiente de forma privilegiada sem necessidade do uso de VPN.
1.14. Gerar vídeos e logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências.

1.15. O CONTRATADO é responsável pela definição, dimensionamento, configuração e parametrização no ambiente da CONTRATANTE, com recursos suficientes para suportar a Solução nos volumes de dados, transações e usuários do CONTRATANTE, nos níveis de disponibilidade e desempenho necessários à mesma.

1.16. A solução deve ser baseada no modelo on premisse em uma das plataformas abaixo:

1.16.1. *appliance virtual*, com sistema operacional customizado e banco de dados embarcado;

1.16.2. servidor virtual, com todas as licenças necessárias da solução, inclusive as licenças do sistema operacional, exceto as licenças para a infraestrutura de virtualização e banco de dados caso seja Microsoft SQL Server Enterprise (Partnumber: 7JQ-00341);

1.16.3. computador servidor físico, com todas as licenças necessárias da solução, inclusive as licenças do sistema operacional, exceto banco de dados caso seja Microsoft SQL Server Enterprise (Partnumber: 7JQ-00341);

1.16.3.1. caso o computador servidor seja físico, deverá possuir as seguintes configurações mínimas:

1.16.3.1.1. alimentação elétrica em tensão de 110v a 240v com seleção automática;
1.16.3.1.2. deve possuir fontes de alimentação redundantes;
1.16.3.1.3. deve possuir conexões de rede Ethernet redundantes;
1.16.3.1.4. deve possuir sistema de refrigeração/ventilação redundantes;
1.16.3.1.5. deve possuir sistema de armazenamento que implemente RAID1, RAID5 ou superior;
1.16.3.1.6. deve ser montável em rack padrão de 19'' (dezenove polegadas);
1.16.3.1.7. deve possuir no máximo 2U (duas unidades de rack) de altura;
1.16.3.1.8. devem ser fornecidos todos os cabos, trilhos e demais acessórios necessários à montagem, alimentação e disponibilização do equipamento.

1.17. A solução, independentemente da plataforma utilizada, deverá estar atualizada e com suporte ativo de Sistema Operacional e Banco de Dados.

1.18. O serviço quanto a atualização, reparo e assistência de Sistema Operacional e Banco de Dados, fica a cargo do CONTRATADO.

1.19. A solução deve comtemplar, no mínimo, três perfis de acesso para usuário, são eles:

1.19.1. Usuários com acesso à dispositivos geridos pela solução
1.19.2. Usuários com perfil de auditor
1.19.3. Usuários com acesso remoto seguro (suporte)

1.20. A solução deve ter suporte para ambiente devops e ser capaz de gerenciar os segredos/chaves das aplicações pertencentes ao banco.

2. REQUISITOS TECNOLÓGICOS DA SOLUÇÃO

2.1. METODOLOGIA DE ACESSO AOS SITEMAS ALVO

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

2.1.2. Deve prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo.

2.1.3. Deve ser possível habilitar e desabilitar a opção de acesso a partir da utilização da cópia de senha para a tela de login do sistema/aplicação;

2.1.4. Deve ser composto por cofre de senhas, elemento responsável pela geração, revogação, versionamento, armazenamento e controle das credenciais de acesso, e por gateway ou

proxy de sessão, elemento responsável pelo provimento do acesso privilegiado, monitoramento e controle de sessão e modulo de acesso remoto privilegiado;

2.1.5. Deve possuir modulo de gestão de senhas administrativas licenciado juntamente com o cofre de senhas

2.2. INTEGRAÇÃO COM SERVIÇOS DE NUVEM

2.2.1. Deve gerenciar credenciais de ambientes virtualizados baseados em VMware ESXi, RedHat KVM, Microsoft Hyper-V, Microsoft Azure, Amazon Web Services e OpenStack;
2.2.2. Deve gerenciar credenciais do Microsoft Office 365;
2.2.3. Deve ser totalmente compatível com sistemas, serviços e aplicações executando sobre Docker Containers.
2.2.4. Deve realizar o upload de arquivos como certificados, chaves de API, tokens e etc., para o cofre da solução de forma segura e auditada.
2.2.5. Deve realizar a funcionalidade de gerenciamento e armazenamento para sincronização de segredos para DevOps, com capacidade de se conectar e recuperar segredos do Cofre de forma automática.
2.2.6. A solução deve gerenciar segredos para software e máquinas gerenciados, armazenados e recuperados programaticamente por meio de APIs e SDKs (isso inclui gerenciamento de segredos para aplicativos, técnicas de injeção de credenciais e requisitos adicionais de autenticação).
2.2.7. Deve possuir funcionalidade de geração de senhas, baseadas em políticas corporativas;

2.3. INTERFACE WEB

2.3.1. Deve disponibilizar interface Web para administração, gerenciamento e utilização da solução;
2.3.2. A interface Web deve ser compatível com, no mínimo, 02 (dois) dos seguintes navegadores: Google Chrome, Firefox, Microsoft Edge e Internet Explorer;
2.3.3. A interface Web deve suportar a utilização de certificados digitais válidos pela ICP-Brasil e certificados gerados pela ICP-BNB ou auto-assinados gerados pela própria solução
2.3.4. A solução deve suportar o uso de um certificado válido assinado por CA que valide seu endereço de acesso à ferramenta ou suportar o uso da autoridade certificadora "Let's Encrypt" para obter um certificado válido;
2.3.5. A interface Web deve disponibilizar relatórios gráficos no mínimo com as informações gerenciais de:

2.3.5.1. quantidade de credenciais gerenciadas;
2.3.5.2. as credenciais mais utilizadas por período;
2.3.5.3. as credenciais com mais tempo que não alteraram senha;
2.3.5.4. as credenciais nunca usadas;
2.3.5.5. Usuários que mais consultaram credencias.

2.3.6. Deve possuir menu de ajuda em idioma inglês (US) ou português (BR).

2.4. AUTENTICAÇÃO DE USUÁRIOS

2.4.1. Deve realizar autenticação integrada com o Active Directory (AD), não sendo necessária utilização de base local de usuário da solução;

2.4.2. Deve suportar repositório de autenticação com usuários locais;
2.4.3. Deve identificar tentativas de acesso inválidas;
2.4.4. Deve implementar segundo fator de autenticação para os usuários e administradores da solução, a partir da própria solução ou através de integração com terceiros;
2.4.5. Deve prover mecanismos para mitigar ataques de força-bruta;
2.4.6. Deve integrar-se com soluções de autenticação de duplo fator através do protocolo RADIUS, Single Sign on via SAML ou OIDC e Time-Based One-time Password (TOTP);
2.4.7. Deve garantir que os usuários da solução tenham visualização somente dos recursos que tem capacidade de requerer acesso;
2.4.8. Deve automatizar a alocação de acesso entre administradores e suas contas pessoais de administrador;
2.4.9. Deve garantir requisitos de segurança na guarda de credencias, incluindo criptografia no tráfego de informações, suportando, no mínimo, TLS 1.2

2.5. AUTORIZAÇÃO

2.5.1. Deve ter segregação de funções, baseado em perfis de utilização;
2.5.2. Deve dispor de um modelo de controle de acesso baseado em grupos de usuários.
2.5.3. Deve ter a capacidade de aplicar a segregação de funções, por exemplo, permita que os administradores do Windows vejam apenas as sessões do Windows.
2.5.4. Deve garantir que os usuários da solução tenham visualização somente dos recursos que tem capacidade de requerer acesso;
2.5.5. O modulo de acesso remoto seguro deve:
2.5.6. Permitir criação de políticas para grupos de usuários para controlar acessos e permissões;
2.5.7. Armazenar em log no sistema informações das sessões (nome e máquina do usuário transferências de arquivos, informações do sistema, duração da sessão);
2.5.8. Armazenar informações detalhadas das sessões de acesso;

2.6. CONTROLE DE ACESSOS PRIVILEGIADOS
2.6.1. Deve seguir o modelo "zero-trust", onde todos os acessos são barrados até que seja permitido especificamente e granularmente;
2.6.2. Deve prover comandos e filtros para bloquear acessos não autorizados;
2.6.3. Deve gerar alertas, advertências e logs por violação de políticas de acessos;
2.6.4. Deve ser capaz de bloquear a sessão de usuários privilegiados que tentem violar tais
2.6.4.1.1. políticas;
2.6.5. Deve desativar contas de usuários que violem políticas;
2.6.6. Deve limitar usuários a sistemas autorizados;
2.6.7. Deve permitir a criação de listas de comandos definidas como white-list de comandos ou black-list de comandos;

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

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

2.6.8.2. Ao acessar um ativo baseado em Linux, injeção de credenciais deve suportar sua utilização em conjunto com o SUDO;
2.6.8.3. A fim de proteger contra erros comuns do usuário durante as sessões SSH, solução deve suportar filtro de comandos, para bloquear alguns comandos e permitir

que outros, em um esforço para evitar que o usuário inadvertidamente use um comando que pode causar resultados indesejáveis

2.6.8.4. A solução deve realizar o bloqueio da sessão do usuário caso um comando não permitido seja executado durante a sessão

2.7. ESCALADA DE PRIVILÉGIOS

2.7.1. Deve ser configurada para bloquear a escalada de privilégios sem a necessidade de agente instalado na máquina do usuário de origem;
2.7.2. Deve ser capaz de bloquear, detectar e notificar atividades de movimentos laterais de ganhos de privilégios de qualquer forma possível.
2.7.3. Deve ter a capacidade de rastrear atividades de usuários privilegiados e acesso à identidade do usuário original para garantir que os requisitos de responsabilidade sejam atendidos

2.8. FLUXO DE APROVAÇÃO DE ACESSOS

2.8.1. Deve permitir a criação de fluxo de aprovação de acessos às credenciais, com no mínimo as funcionalidades relacionadas abaixo ou integrar-se com o fluxo de aprovação da solução de Helpdesk (Gerenciamento de Serviço) CA SDM – Service Desk Management, a integração pode ser feita via API.

- Políticas de acessos pré-aprovados;
- Políticas de acessos com aprovação única;
- Políticas de acessos com aprovação dupla;
- Políticas de acessos com aprovação única ou dupla de uma relação com vários aprovadores.
- Políticas de acessos por período de tempo;

2.8.2. Deve permitir a rastreabilidade do fluxo de aprovação de acessos com logs;
2.8.3. Deve permitir a criação de fluxos customizáveis de aprovação de acesso privilegiado, garantindo os seguintes aspectos:
2.8.3.1. Configuração de acessos pré-aprovados;
2.8.3.2. Interface para solicitar e aprovar acessos, com exposição do motivo;
2.8.3.3. Notificação em casos de acessos não aprovados para solicitantes.
2.8.3.4. Exigir aprovação antes do início de uma sessão, suportando no mínimo uma notificação por e-mail de aprovação enviado aos destinatários designados sempre que uma tentativa de sessão com qualquer ativo. Solicitando que o usuário insira um motivo da solicitação, a hora e a duração da solicitação.

2.9. GERENCIA DE ACESSOS EM APLICAÇÕES

2.9.1. A solução deve obrigatoriamente, de forma nativa ou API, prover mecanismos para que os arquivos de linha de comando (por exemplo, scripts .bat, CMD, .sh, Powershell, vbs, KIX e outros) possam "utilizar" senhas das contas privilegiadas administradas pela solução com retirada e devolução da credencial), de modo a eliminar a necessidade de senhas internalizadas em tais arquivos;
2.9.2. Deve fornecer serviços de API's para realizar a solicitação e devolução de credenciais;
2.9.3. Deve gerir as contas privilegiadas de modo a garantir que a troca automática destas senhas não interfira na utilização destas contas;

2.9.4. Deve prover mecanismos para que as contas privilegiadas administradas pela solução em uso com aplicações possam ser auditadas e constem nos relatórios;
2.9.5. Deve gerenciar credenciais de aplicações, eliminando senhas internalizadas em códigos fonte de programas de computadores ou scripts de comandos;
2.9.6. Deve fornecer acesso simultâneo para no mínimo dois usuários ao mesmo dispositivo, sem comprometimento da rastreabilidade;
2.9.7. Deve prover a funcionalidade de entrega de sessão autenticada no dispositivo-alvo, iniciada com sucesso, sem que o requerente tenha contato com a senha daquele sistema ou dispositivo;
2.9.8. Deve possibilitar realizar o login automático no dispositivo gerenciado (ou dispositivo-alvo) usando credenciais privilegiadas sem revelar aos usuários tais credenciais;
2.9.9. Deve operar como proxy de conexões via SSH/TELNET para qualquer dispositivo gerenciado, através de clients SSH tais como PuTTy, MobaXTerm, secureCRT e outros;
2.9.10. Suportar o acesso externo a rede sem qualquer necessidade de utilização de VPN ou método similar de acesso
2.9.11. Permitir o acesso remoto, no mínimo, aos seguintes sistemas:
  2.9.11.1. Microsoft, Desktop e Servidores;
  2.9.11.2. Linux Red Hat Enterprise e similares;
  2.9.11.3. VNC (para ambientes legados e ambientes de automação – IoT);
  2.9.11.4. Mainframe por meio de terminal.
2.9.12. Utilizar protocolos de comunicação fazendo uso de criptografia TLS 1.2 ou superior;
2.9.13. Suportar o funcionamento a redes que não estão conectadas diretamente a internet e a redes seguras;
2.9.14. Suportar o acesso sem necessidade de permissão prévia para o acesso a desktops e servidores;
2.9.15. Possibilitar o acesso a dispositivos de rede via SSH, como roteadores e switches;
2.9.16. Disponibilizar aos usuários, console de acesso Web para a solução, sem a necessidade de instalação de plug-ins ou agentes;
2.9.17. Deve prover conexões RDP controladas por meio de um JUMP SERVER;
2.9.18. Deve possibilitar que a console do Microsoft SQL Server Management Studio (SSMS) seja disponibilizada para os usuários de forma controlada e auditada; O acesso à console do SSMS deve ser configurável, de maneira a impedir que seja possível conectar-se de forma não autorizada a bases de dados e objetos do Microsoft SQL Server hospedados em computadores servidores para os quais não foram solicitadas credenciais de acesso.
2.9.19. A solução deverá realizar a troca automática da senha da ligação entre servidores MS SQL Server com as aplicações conectadas
2.9.20. Suportar provedores externos de identidades para autenticação, incluindo, no mínimo, servidores LDAP, Active Directory, RADIUS e Kerberos, bem como atribuir privilégios com base na hierarquia e nas configurações de grupo já ´ especificadas nos respectivos servidores;
2.9.21. Integrar-se com soluções de autenticação de duplo fator através de protocolo RADIUS, Single Sign-on via SAML ou OIDC e Time-Based One-Time Password (TOTP);
2.9.22. Suportar o uso de um certificado assinado por uma autoridade certificadora válida;
2.9.23. Permitir o agendamento para liberação do acesso remoto, incluindo notificação por e-mail aos destinatários designados;
2.9.24. Permitir forçar o encerramento da sessão remota pelo supervisor, com notificação ao cliente;
2.9.25. Prover monitoramento ao vivo e gravação da sessão, com registro completo das atividades executadas durante a sessão executada pelos usuários;
2.9.26. Permitir que cada usuário trabalhe em múltiplas sessões ao mesmo tempo, independentemente da plataforma dos clientes atendidos

2.9.27. Limitar o acesso a aplicativos especificados no sistema remoto, incluindo a acesso a área de trabalho remota;
2.9.28. 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
2.9.29. Suportar filtro de comandos durante as sessões SSH, visando evitar que o usuário inadvertidamente use um comando que pode causar danos ao servidor acessado;
2.9.30. Suportar a injeção automática de credenciais em sistemas Windows, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a ação de "executar como";
2.9.31. Suportar a injeção automática de credenciais em sistemas Unix/Linux, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a utilização em conjunto com o sudo;
2.9.32. A solução deve poder operar de forma autônoma, sem a necessidade de integração com soluções de cofre de senhas para armazenar os ativos, segredos e credenciais, caso seja necessário;

2.10. GERENCIAMENTO DE CREDENCIAIS

2.10.1. Deve realizar a descoberta na rede de utilização das credenciais;
2.10.2. Deve automatizar a alteração de senhas, chaves de sessão SSH e outras credenciais;
2.10.3. Garantir requisitos de segurança na guarda de credenciais, incluindo criptografia no tráfego de informações, suportando no mínimo TLS 1.2
2.10.4. Deve armazenar credenciais sempre em modo seguro e criptografado, protegendo-as com chave-mestre com nível de segurança alto, seja via software ou sobre um HSM FIPS-140.2;
2.10.5. Deve escalar até 1.000 (hum mil) credenciais (entre sites ou ambientes híbridos da arquitetura) sem perda de qualidade de acesso;
2.10.6. Deve gerenciar senhas privilegiadas de aplicações, de modo a evitar que sejam senhas estáticas em códigos-fonte (hardcoded), garantindo os seguintes aspectos:
- Solicitação de credenciais via REST sob demanda ao invés de credenciais estáticas;
- Atualização automática de contas no banco de dados de senhas;
- Inscrição automática de sistemas alvo sem aguardar por atualizações dinâmicas;

2.10.7. Deve possuir configurações de segurança que garantam o acesso apenas por aplicações permitidas, suportando no mínimo o endereço de origem das requisições, nome de usuário, autenticação por certificados e/ou caminho da aplicação.
2.10.8. Deve gerenciar e modificar credenciais conforme as necessidades, baseando-se sempre nas políticas de mudanças de senha, incluindo a rotação de senhas nos dispositivos gerenciados (alvos) em intervalos regulares parametrizados na solução;
2.10.9. Deve forçar a devolução da senha de uma conta privilegiada;
2.10.10. Deve centralizar, administrar, armazenar, liberar e auditar credenciais;
2.10.11. Deve disponibilizar o recurso "break glass" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade.
2.10.12. A solução deve ser capaz de realizar a integração de forma automatizada de contas e permissões aos seus recursos;
2.10.13. Deve realizar o gerenciamento de credenciais, em que credencial é qualquer senha, chave criptográfica ou token capaz de ser guardado de maneira segura, garantindo os seguintes aspectos:
2.10.13.1. Rotatividade de credenciais, permitindo a geração de senhas aleatórias para ativos e grupo de ativos;

2.10.14. Deve ser possível revogar as credenciais sob demanda ou por meio de política definida;
2.10.15. Especificação do tipo de caracteres para a composição de senhas, incluindo caracteres alfabéticos maiúsculos, minúsculos, numéricos, especiais e símbolos, por ativos ou grupo de ativos;
2.10.16. Definição de tempo de validade de credencias;
2.10.17. Criptografia de credencias com protocolos padrões da indústria, incluindo AES 256;
2.10.18. Capacidade de reinicialização de serviços e dependências, no caso de mudança de uma credencial de serviço;
2.10.19. Segmentação de senhas, por autorização de múltiplos aprovadores;
2.10.20. Possuir funcionalidade de discovery, capaz de buscar e registrar novos ativos alvo, garantindo as seguintes condições:
2.10.20.1. Capacidade de realizar buscas no Active Directory e em blocos de endereços IP, podendo ser realizada por demanda, agendada e rotina periódica;
2.10.20.2. Capacidade de especificar o DN ao pesquisar usuários no servidor LDAP;
2.10.20.3. Levantamento de contas administrativas em cada ativo;
2.10.20.4. Levantamento de ativos e de suas respectivas identidades em grupos, de acordo com parâmetros previamente configurados;
2.10.20.5. Classificação automática de contas locais e de domínio;
2.10.20.6. Identificação de contas de serviços e de tarefas em ambientes Microsoft Windows;
2.10.20.7. Identificação de portas abertas nos sistemas descobertos;
2.10.20.8. Identificação de aplicações instaladas em servidores Windows descobertos;
2.10.20.9. Identificação de contas locais e que possuam chaves SSH em ambientes Unix/Linux;
2.10.21. A solução deve ser capaz de criar contas locais em servidores Linux a partir de console Web centralizada, de forma a acelerar o processo de implantação da solução de Cofre de Senhas em ambientes Linux;
2.10.22. A solução deverá suportar a execução de scripts no ambiente Linux e Windows a partir de console Web centralizada;
2.10.23. A solução deve ser capaz gerenciar contas em vários domínios do AD. As contas a serem gerenciadas devem incluir Conta de administrador padrão do domínio, contas locais no servidor/estação de trabalho, SQL Server Admin (SA) e contas privilegiadas do Azure AD;
2.10.24. Deve possuir extensão de navegador que permita, além de credenciais e senhas.
2.10.25. A extensão de navegador deve ser disponibilizada, no mínimo, nos seguintes idiomas: Inglês e português
2.10.26. Deve ser possível através do campo de formulário de um site possuir opção de injetar automaticamente o usuário e a credencial, copiar a credencial e copiar o usuário protegidos pela extensão de navegador
2.10.27. Deve permitir que o usuário organize suas credenciais por pastas, sem a necessidade de contactar o administrador do produto, através da extensão de navegador;
2.10.28. A extensão deve permitir o sincronismo automático do plugin com o cofre de senhas, assim como a sincronização manual;
2.10.29. Deve através da extensão do navegador ser capaz de listar as credenciais disponíveis para o mesmo site;
2.10.30. Deve ser possível também adicionar novas credenciais a partir da extensão de navegador para o site cadastrado sem a necessidade de acesso ao cofre de senhas;
2.10.31. Deve ser possível realizar as seguintes ações através da extensão de navegador:
2.10.31.1. Criar uma credencial;
2.10.31.2. Atualizar uma credencial;

2.11. AUDITORIA

2.11.1. Deve gerar uma trilha de auditoria, com no mínimo os seguintes eventos:

- data e hora de início e fim da sessão.
- tempo de sessão.
- identidade do usuário;
- tipo do evento,
- históricos de acessos;
- eventos realizados na sessão.

2.11.2. Deve disponibilizar relatório dos logs, no mínimo, com as seguintes possibilidades de filtros:

- usuário;
- conta privilegiada;
- sistema-alvo acessado;
- intervalo de tempo (data/hora/minuto inicial e final).

2.11.3. Deve gerar relatório das trilhas de auditoria de modo que sejam compreensíveis pelo usuário (sem necessidade de software adicional para leitura).

2.11.4. Deve proibir a leitura das trilhas de auditoria por usuários não autorizados e não deve ser passível de quaisquer alterações por parte dos usuários privilegiados.

2.11.5. Deve disponibilizar um perfil de auditor com permissão de acesso, no mínimo, para visualizar política de credenciais de acesso, logs, trilha de auditoria, relatórios e gravações.

2.12. INTEGRAÇÕES SISTÊMICAS

2.12.1. Deve prover integração com repositórios padrão Active Directory, LDAP e OpenLDAP:

2.12.1.1. manter o controle de retirada e devolução de senha de acesso privilegiado (Check in e Check out);

2.12.1.2. trocar da senha de uma conta de forma automática;

2.12.1.3. manter a lista de ativos por cadastro ou regra (ex: ID único da máquina, FQDN ou IP);

2.12.1.4. deve ser capaz de localizar automaticamente novos dispositivos instalados na rede e gerenciar as credenciais desses equipamentos;

2.12.1.5. deve ser totalmente compatível com os protocolos de comunicação de rede IPv4 e IPv6;

2.12.1.6. deve ser possível sincronizar a data do sistema a partir de Servidor de Tempo (NTP Server) da rede local e rede externa, dependendo da necessidade do Banco.

2.12.2. Deve permitir a integração com certificados PKI/X.509 e tokens de segurança.

2.12.3. Deve suportar acesso a dispositivos Linux/Unix por meio de SSH ou Telnet, Microsoft Windows e aplicações publicadas via RDP, banco de dados através da console de gerenciamento do fabricante do SGBD, sistemas mainframe como TN3270 ou TN5250 e também dispositivos de rede e segurança que possuam conectividade via SSH e Telnet.

2.12.4. Deve possibilitar que um Hardware Security Module (HSM) seja integrado para armazenamento externo e seguro de chaves conforme as necessidades da solução.

2.12.5. Deve suportar a execução local de aplicações, invocando conexões de aplicações locais/desktop em dispositivos gerenciados.
2.12.6. Deve permitir integração por meio de webservices ou APIs programáveis.
2.12.7. Deve integrar-se com soluções de SIEM (Security Incident Event Management) para análise e correlação de eventos.
2.12.8. Deve integrar-se, de forma nativa ou API, com solução de Helpdesk (Gerenciamento de Serviço) CA SDM — Service Desk Management vigente no BANCO, consumindo os webservices expostos para verificação de chamados, criação de chamados e retornos.

2.13. GRAVAÇÃO DE SESSÃO

2.13.1. Deve realizar a gravação em vídeo e logs de texto das atividades dentro das sessões realizadas pelos usuários nos sistemas-alvo.
2.13.2. Deve realizar a gravação em vídeo e logs de texto das sessões simultâneas.
2.13.3. Deve possibilitar a parametrização dos dispositivos e as contas privilegiadas que terão à sessão gravada.
2.13.4. Deve prover mecanismo de busca de gravações registradas, no mínimo, com as seguintes possibilidades de filtros:

- usuário;
- conta privilegiado;
- sistema-alvo acessado;
- tipo de atividade;
- intervalo de tempo (data/hora/minuto inicial e final).

2.13.5. Deve realizar monitoração da sessão em tempo real, com possibilidade de encerrá-la.
2.13.6. Deve armazenar os vídeos na solução durante o período mínimo de 06 meses, podendo utilizar ferramentas integradas para esta finalidade; neste caso a ferramenta deve fazer parte da solução.
2.13.7. Deve possibilitar que os dados armazenados sejam migrados para armazenamento fora da Solução para fins de arquivamento.
2.13.8. Realizar a gravação da sessão sem a necessidade de nenhum software ou agente pré-instalado no sistema alvo;
2.13.9. Deve ao fechar a sessão deslogar o usuário conectado;
2.13.10. Ser capaz de monitorar sessões, gravar sessões, capturar telas, coletar, armazenar e indexar logs de teclas pressionadas em teclado (keystrokes) em acessos privilegiados, garantindo os seguintes requisitos:

2.13.10.1. Alerta ao usuário privilegiado que a sessão está sendo gravada;
2.13.10.2. Monitoramento por meio de gravação de vídeos, em formato padrão de execução da solução;
2.13.10.3. Monitoramento ao vivo, permitindo ao usuário supervisor, previamente configurado, realizar ações de lock/unlock, suspender e terminar a conexão;
2.13.10.4. Pesquisa avançada de eventos de segurança em todas as sessões gravadas, incluindo comandos digitados, copiar e colar arquivos e execução de softwares;
2.13.10.5. As funcionalidades de gerenciamento e monitoramento de sessões devem impedir que os usuários executem determinadas ações durante uma sessão e ser capaz de executar ações automaticamente na detecção de eventos de sessão configurados nas políticas de acesso. (Ex. Suspender a sessão do usuário);

2.13.11. Deverá ter a capacidade de registrar sessões privilegiadas e armazená-las de forma segura em um repositório criptografado e inviolável. A gravação da sessão não deve afetar o desempenho do dispositivo de destino
2.13.12. Controlar e monitorar sessões usando protocolos padrões e acesso remoto, incluindo RDP, HTTP/HTTPS e SSH;

2.14. SEGURANÇA

2.14.1. Deve possuir armazenamento de dados embarcado ou com software de mercado, incluindo todo o licenciamento de software necessário à sua utilização.
2.14.2. Deve prover mecanismos de criptografia para informações sensíveis armazenadas em banco de dados.
2.14.3. Deve prover os seguintes padrões criptográficos por determinadas funcionalidades:

2.14.3.1. algoritmo AES-256 para criptografia do tráfego de informações;
2.14.3.2. FIPS-140.2;

2.14.4. Deve armazenar credenciais de forma criptografada.
2.14.5. Deve ser compatível ou prover solução de canal seguro SSL 3.0/TLS 1.0'.
2.14.6. Deve suportar certificados digitais com chave igual ou superior a 2048 bits.
2.14.7. Deve possuir mecanismos para evitar acessos indevidos e bloqueio de acessos classificados como tentativas de invasão por força bruta.
2.14.8. Deve ter controle da complexidade de senha por meio de uma política configurável.
2.14.9. Deve armazenar as contas e senhas privilegiadas em um repositório seguro e criptografado.
2.14.10. Deve ser capaz de bloquear sessões de operadores em casos de incidentes de segurança.
2.14.11. 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.
2.14.12. Deve gerar alerta para os administradores em casos de incidentes de segurança.
2.14.13. Deve criptografar toda a transmissão de dados entre os componentes da solução.
2.14.14. Deve permitir configurar o nível de complexidade das senhas geradas, com opções de definição de comprimento e tipo de caracteres que comporão essas senhas.
2.14.15. Deve possuir inteligência de forma a impedir que as senhas modificadas se repitam para a mesma credencial gerenciada, sendo a quantidade de repetições definida em normativo de segurança.
2.14.16. Deve ser possível gerar alertas em caso de falha de troca de senha.

2.15. RELATÓRIOS

2.15.1. Deve disponibilizar os relatórios somente para os usuários autorizados pelo administrador da solução.
2.15.2. Deve disponibilizar relatório para rastrear a utilização de contas privilegiadas no ambiente computacional.
2.15.3. Deve possuir mecanismos para geração de relatórios pelo administrador de relatórios.
2.15.4. Prover relatórios de auditoria que disponibilizem informações das interações dos usuários, tais como atividades de login, adição e remoção de senhas privilegiadas, endereço IP de máquina de origem e do destino alvo, atividades administrativas de

delegação e revogação de acesso e eventos agendados. Os relatórios devem ser filtrados por período, tipo de operação, sistema e usuários;

2.15.5. Deve gerar relatórios baseados nos logs.
2.15.6. Deve ser possível gerar relatórios em um dos formatos: CSV, XLS, XLSL, PDF, HTML.
2.15.7. Prover relatórios de conformidade que disponibilizem operações, incluindo lista de sistemas gerenciados, eventos de alteração de senha, auditoria de contas e alertas de segurança

2.16. MONITORAMENTO

2.16.1. Deve disponibilizar comunicação SNMP.
2.16.2. Deve implementar a MIB II, conforme RFC 1213.
2.16.3. Deve integra-se com a solução de monitoramento da CA, de forma nativa ou API.

2.17. BACKUP E RESTORE

2.17.1. Deve permitir o backup da base de dados da solução e todas as suas configurações.
2.17.2. Dever permitir o restore, base de dados da solução.
2.17.3. Deve permitir salvar o backup para fins de arquivamento na ferramenta de backup Veeam Backup Restore
2.17.4. Deve possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha para recuperações de senhas no caso de falha total da solução.
2.17.5. Deve possuir sistema de backup e restore que permita o administrador realize o agendamento de data e horário para a execução de tarefas de salvaguarda e recuperação de dados.
2.17.6. Deve permitir a realização do backup de maneira automática ou por agendamento;
2.17.7. Os requisitos de backup e restore devem funcionar tanto no site primário quanto no site secundário.

2.18. CONTINGÊNCIA

2.18.1. Deve funcionar em modo de alta disponibilidade, com cluster ativo – ativo, no sítio primário e no sítio secundário com redundância da base de dados entre os sítios.
2.18.1.1. Caso a solução ofertada, com cluster ativo-ativo, necessite de uma base da dados SQL Server (Partnumber: 7JQ-00341) para funcionamento, O CONTRANTE fornecerá os recursos necessários para implementação da solução
2.18.2. No caso de falha de um dos servidores do cluster da solução, cada um dos servidores deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ou nas funcionalidades.
2.18.3. O sítio secundário pode funcionar ativo – ativo com o sítio primário ou somente em caso de recuperação de desastres.
2.18.4. Os dados devem ser sincronizados automaticamente entre o sítio primário e secundário.

2.19. DEVOPS

2.19.1. A solução deverá ser capaz de realizar o armazenamento seguro e gerenciamento central de credenciais e segredos (secrets) como senhas, chaves de API e para fluxos de

trabalho DevOps, sem a necessidade de incorporar ou codificar senhas ou outros segredos dentro de códigos ou scripts;

2.19.2. A solução de software deve ser capaz de armazenar e gerenciar segredos dos tipos: secret certificado e secrets do tipo texto ou string. Qualquer string que deva ser mantido confidencial, ou chave de criptografia, ou senha, ou token, será considerado um segredo, a ser gerenciado pela solução, considerando ambientes DevOps;

2.19.3. A solução deverá ser capaz de alternar credenciais com base em políticas de configuração;

2.19.4. A solução deve ser capaz de permitir o uso dos segredos (secrets) através de APIs sem expor na stack de configuração eliminando credenciais embarcadas nas aplicações;

2.19.5. A Solução deve permitir a integração nativa ou através de API, com ferramentas DevOps como: Ansible, Azure DevOps, Jenkins, Gitlab, Kubernetes e Puppet;

2.19.6. A solução deve possuir trilha de auditoria de todas as operações de segredos e capacidade de auditar todo o ciclo de vida dos segredos.

2.19.7. Todos os registros de eventos de segurança como autenticação de clientes, solicitação de segredos, revogação de segredos, acesso de usuários, aplicações ou clientes a segredos, mudanças de permissão, deverão ser armazenados de maneira que impossibilite a sua alteração e se mantenha a correta integridade das evidências.

2.19.8. A solução deve atuar como intermediária de segredos para diversos clientes como aplicações, contêineres e clientes de criptografia.

2.19.9. O fornecimento de segredos deve oferecer meios de controle de solicitante com múltiplos fatores, incluindo restrições de IP/range.