DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

PROA: 23/1400-0012119-4

Requerente: Departamento de Tecnologia da Informação e Comunicação

Assunto: Solução de Gerenciamento de Acesso Privilegiado

ANEXO II

TERMO DE REFERÊNCIA - TR

1. OBJETO:

1.1. Contratação de Solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management - PAM), incluindo licenciamento com prazo de 5 anos e serviço de implantação conforme definido no item 3.2, podendo ser prorrogável pelo prazo máximo de 10 anos.

2. FUNDAMENTAÇÃO / JUSTIFICATIVA:

2.1. Conforme plano de contratação descrito no Estudo Técnico Preliminar (ETP), a DETIC da SEFAZ-RS, buscando atingir seus objetivos estratégicos relacionados à segurança da informação, necessita adquirir soluções para gestão de acessos privilegiados. De acordo com as boas práticas, normas e recomendações técnicas de diversas entidades, o Gerenciamento de Acesso Privilegiado visa mitigar riscos de TI e consequentemente os riscos operacionais envolvidos nos processos de sustentação dos serviços.

2.2. Diante do exposto, a pretensa aquisição justifica-se pelo anseio em melhorar a gestão de controle dos acessos a contas privilegiadas e genéricas, viabilizando a rastreabilidade dos responsáveis por atos praticados com suas credenciais, inclusive o tempo em posse e uso da conta, do fornecimento de senhas temporárias e do registro de tudo o que foi feito durante as sessões abertas, preservando evidências e garantindo a auditabilidade.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

2.3. A contratação da solução de Gerenciamento de Acesso Privilegiado, tem como metas:

2.3.1. Manter as contas privilegiadas em um único repositório seguro;

2.3.2. Implementar regras para autorização do uso das contas privilegiadas;

2.3.3. Geração automática da senha no momento da retirada;

2.3.4. Entrega de sessão autenticada, sem que o usuário tenha contato com a senha;

2.3.5. Definir o tempo em que o usuário autorizado poderá usufruir da conta privilegiada;

2.3.6. Registrar as ações realizadas em posse de conta privilegiada com possibilidade de gravação de sessão (gravação de telas);

2.3.7. Melhorar controle sobre a utilização de recursos privilegiados do ambiente computacional;

2.3.8. Obter o monitoramento das ações de funcionários e terceiros com o uso de credenciais privilegiadas;

2.3.9. Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;

2.3.10. Melhorar qualidade na prestação de informações aos órgãos de controle;

2.3.11. Rastrear o uso de contas privilegiadas no ambiente computacional;

3. ESPECIFICAÇÃO DO PRODUTO/ SERVIÇO:

Lote	Item	Descrição	Quantidade	GCE
1	1	Solução de Gerenciamento de Acesso Privilegiado, com fornecimento de Licenças por subscrição, pelo período de 60 meses	1	0035.0736.010136
	2	Serviços		
	2.1	Serviço de Treinamento	1	0035.1000.000007

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

	2.2	Serviço de Implantação	1	0035.1000.000008
	2.3	Serviço em Horas Técnicas	200 Horas	0035.1000.000009

3.1. **Solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management - PAM), com licenciamento por subscrição para 60 (sessenta) meses**.

3.1.1. Por definição é um conjunto de softwares que operando em conjunto e de forma harmônica compõem a Solução de Gerenciamento de Acesso Privilegiado para controle da segurança de identidade que contribui com a proteção contra ameaças cibernéticas ao monitorar, detectar e impedir o acesso privilegiado não autorizado a recursos críticos. Mais detalhes quantos aos requisitos da SEFAZ-RS estão disponíveis no “Anexo A – Premissas do Projeto”.

3.1.2. Deverá estar licenciada para uso para as seguintes quantidades dos respectivos tipos de usuários:

3.1.2.1. Usuários Nominais: 140
3.1.2.2. Usuários Administrativos: 10
3.1.2.3. Usuários de Serviços: 10
3.1.2.4. Ativos de Rede: 10
3.1.2.5. Estações de Trabalho: 10
3.1.2.6. Servidores Windows: 345
3.1.2.7. Servidores Linux: 70

3.1.3. **Usuário Administrativos – 10 unidade(s)**

3.1.3.1. Compõe o licenciamento baseado no número de usuários que utilizem contas que requerem elevação de privilégio de acesso ao sistema de administração da solução.

3.1.4. **Usuário Nominal – 140 unidade(s)**

3.1.4.1. Compõe o licenciamento baseado no número de usuários que utilizem contas comuns no ambiente on-premisse que não possuem elevado privilégio de acesso ao sistema de administração da solução.

3.1.5. **Dispositivos de Rede - 10 unidade(s)**

3.1.5.1. Licenciamento baseado em número de dispositivos de rede para realização de troca de senha automáticas.

3.1.6. **Estações de Trabalho - 10 unidade(s)**

3.1.6.1. Licenciamento baseado em número de estações de trabalho para realização de troca de senha automáticas.

3.1.7. **Servidores Windows - 345 unidade(s)**

3.1.7.1. Licenciamento baseado em número de servidores físicos e virtuais com sistema operacional Windows Server de trabalho para realização de troca de senha automáticas.

3.1.8. **Servidor Linux - 70 unidade(s)**

3.1.8.1. Licenciamento baseado em número de servidores físicos e virtuais com sistema operacional Linux de trabalho para realização de troca de senha automáticas.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.1.9. **Administração**

3.1.9.1. A solução deverá possuir todas as funções fornecidas pelo mesmo fabricante, sem dependência de ferramentas de terceiros ou adaptações.

3.1.9.2. Possibilidade de comunicação com os serviços de diretório via protocolo LDAPS.

3.1.9.3. Suportar sincronização do relógio interno via protocolo NTP.

3.1.9.4. A solução deve possuir interface única, na mesma solução, para o gerenciamento de senhas e sessões.

3.1.9.5. A solução deve oferecer o provisionamento e gerenciamento de todas as contas privilegiadas, incluindo contas para a administração de aplicações de negócio, bancos de dados e dispositivos de redes, não se limitando apenas às contas de sistemas operacionais de servidores.

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

3.1.9.7. A solução deverá prover mecanismos de atualização de segurança.

3.1.9.8. Ter uma console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas.

3.1.9.9. A CONTRATADA deverá arcar com todos os custos de licenciamento para o gerenciador de banco de dados que requeira, garantindo total compatibilidade das funcionalidades da solução requeridas nas especificações elaboradas pela CONTRATANTE.

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

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

3.1.9.12. Permitir a execução de backups automatizados através da programação/agendamento.

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

3.1.9.14. Extrair backups do sistema, logs e vídeos além das credenciais para um servidor localizado em Data Centers remotos caso seja necessário para restaurar todas as configurações e os dados da solução de cofre de senhas.

3.1.9.15. A solução deve permitir que você finalize todas as sessões em andamento, bloqueie o acesso a dispositivos predefinidos ou bloqueie todo o acesso a ele por um período definido.

3.1.9.16. Todo licenciamento adicional para operação em Alta Disponibilidade das máquinas virtuais da Solução deverá ser custeado pela CONTRATADA.

3.1.9.17. Caso necessitem de máquinas virtuais adicionais para execução de serviços acessórios a solução que permitam a garantia da Alta Disponibilidade, serão aceitos apenas os que operem com os Sistemas Operacionais Licenciados Windows Server 2022 ou Red Hat Enterprise Linux 9 ou de suas respectivas versões superiores.

3.1.9.18. A solução completa deverá operar com suporte a Alta Disponibilidade.

3.1.10. **Gerenciamento de senhas**

3.1.10.1. 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.

3.1.10.2. Gerenciar chaves SSH e fazer varredura de servidores Linux bem como a identificação e publicação de chaves SSH.

3.1.10.3. Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;

3.1.10.4. Consolidação periódica de senhas para identificar senhas que foram alteradas em sistemas gerenciados.

3.1.10.5. Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legados.

3.1.10.6. Oferecer interface com visão personalizada exclusiva para Auditorias e Órgãos Reguladores, contendo os dispositivos e credenciais gerenciadas pela solução.

3.1.10.7. Fornecer uma área de transferência segura, para que o solicitante possa visualizar ou copiar a senha na tela de login do sistema de destino.

3.1.10.8. Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata.

3.1.10.9. Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais.

3.1.10.10. Permitir o monitoramento on-line do uso das contas e desligamento da sessão.

3.1.10.11. Apresentar o recurso "break glass" para acesso de emergência às contas, ou seja, ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (repositório seguro), para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso a todas as senhas de identidades privilegiadas gerenciadas pela solução.

3.1.10.12. Oferecer a funcionalidade de "Discovery" para realizar busca de novos servidores, elementos de rede e bancos de dados.

3.1.10.13. Possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão caso o usuário execute um comando indevido.

3.1.10.14. Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas.

3.1.10.15. Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiados.

3.1.10.16. Possibilidade de geração de relatórios baseados nos logs e exportá-los para arquivos em formato "CSV".

3.1.10.17. 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, WinRM, SSH, API REST HTTP/HTTPS.

3.1.10.18. As senhas geradas automaticamente pela solução de cofre de senhas devem seguir os seguintes requisitos:

3.1.10.18.1. Poder determinar a quantidade de caracteres;

3.1.10.18.2. Ser composta por números, letras maiúsculas, letras minúsculas e por caracteres especiais;

3.1.10.18.3. Poder ser pré-definidas quais caracteres especiais poderão ser utilizados;

3.1.10.18.4. Aleatórias de modo que dentro do histórico de uma conta seja improvável encontrar duas senhas iguais;

3.1.10.18.5. Não seja baseada em palavra de dicionário.

3.1.10.19. 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 plataformas ou criticidades.

3.1.10.20. As informações com as senhas trocadas e últimas senhas devem ficar salvas e podem ser consultadas nos relatórios de segurança e auditoria, que podem ser exportados por administradores da solução.

3.1.10.21. 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.

3.1.10.22. A solução deve ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos.

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

3.1.10.24. A solução não deverá depender da instalação de agentes para realizar a troca de senhas.

3.1.10.25. 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.

3.1.10.26. A solução deve ter a capacidade de realizar a reconciliação de credenciais automaticamente.

3.1.11. **Rotação de senhas**

3.1.11.1. Troca automática de senhas para Servidores (Unix, Linux, Windows), Bancos de Dados (MS SQL, MySQL, Greenplum, Apache HBase), Aplicações Web, Dispositivos de Rede.

3.1.11.2. A solução deverá realizar a troca automática da senha da ligação entre servidores MS SQL Server com as aplicações conectadas.

3.1.11.3. Geração automática de senhas de força/complexidade de acordo com as regras de cada tecnologia e Política de Segurança da CONTRATANTE;

3.1.11.4. Flexibilidade para configuração de força de senha gerada.

3.1.11.5. Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo.

3.1.11.6. Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado.

3.1.11.7. Armazenamento de histórico de senhas de usuários por equipamento;

3.1.11.8. Registro de troca executadas.

3.1.11.9. Relatório de acompanhamento de trocas.

3.1.11.10. Relatório de erros de trocas.

3.1.11.11. Alertas de falha ou sucesso de trocas.

3.1.11.12. Possibilidade de reconfiguração/customização de scripts ou plugin de troca de senhas para configuração de casos que exijam parâmetros específicos para rotação de senhas.

3.1.11.13. Configuração de políticas de trocas de senhas com agendamento programado ou por ocorrências de eventos com especificação de parâmetros de prazo para a troca.

3.1.11.14. Disponibilizar os Templates de troca de senha de forma que possam ser abertos, editáveis e auditáveis.

3.1.11.15. Templates com linguagem acessível e fácil interpretação.
3.1.11.16. Rastreabilidade de Alteração de Template.

3.1.12. **Controle de Acesso**

3.1.12.1. A solução deve ser capaz de limitar a execução de comandos críticos pelos usuários privilegiados cadastrados.
3.1.12.2. A solução deve ser capaz de prover acesso externo sem a necessidade de instalação de Agent ou utilização de VPN
3.1.12.3. A solução deve permitir o controle de execução de comandos críticos por, pelo menos, “whitelist” e/ou “blacklist”.
3.1.12.4. A solução deve permitir o início e a condução de sessões dentro do próprio navegador ou através de clientes externos como o mstsc.exe e o putty.exe.
3.1.12.5. A solução deve possuir tempo de expiração de sessão configurável pelo administrador do sistema.
3.1.12.6. A solução deve suportar a desconexão da sessão por atividade/uso indevido de comandos pré-cadastrados no sistema.
3.1.12.7. A solução deve permitir a criação de grupos de usuários.
3.1.12.8. Bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução - Baseado em blacklist e/ou whitelist.
3.1.12.9. Possibilidade de bloqueio e auditoria de comandos específicos;
3.1.12.10. Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas.
3.1.12.11. Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado.
3.1.12.12. A solução deve permitir a atribuição de privilégios a grupos de usuários, associados a um ou mais alvos gerenciados.
3.1.12.13. A Solução deve permitir integração com ferramentas de gestão de incidentes (ITSM) para validar tickets abertos durante processo de aprovação de acesso.
3.1.12.14. A solução deve permitir acesso simultâneo ao cofre de senhas e as contas privilegiadas por dois ou mais usuários.
3.1.12.15. A solução deve ser compatível com recursos de segregação de funções entre usuários nas aplicações gerenciadas.
3.1.12.16. A solução deve fornecer funcionalidade para revogar imediatamente todas as sessões remotas para um usuário conectado.
3.1.12.17. A solução deve permitir acesso simultâneo à credenciais privilegiadas por dois ou mais usuários.
3.1.12.18. Acessos simultâneos a credenciais, senhas e dispositivos não devem possuir comprometimento da rastreabilidade.

3.1.13. **Integração e compatibilidade**

3.1.13.1. Possibilitar via script, a criação de novos conectores baseado em acessos SSH e RDP, para que seja possível suportar novas interfaces de autenticação de ativos.
3.1.13.2. A solução deve suportar acesso via dispositivos móveis como tablets e smartphones.
3.1.13.3. A solução deverá permitir o gerenciamento e monitoramento de sessões do Microsoft Azure.
3.1.13.4. Ser compatível com sistemas operacionais: Windows Server 2012 ou superior, Red Hat Enterprise 7 ou superior.
3.1.13.5. Ser compatível com sistemas gerenciadores de bancos de dados: MS SQL, MySQL, Postgres (Greenplum);

3.1.13.6. Ser compatível com appliances de segurança: Fortigate e Aruba ClearPass;
3.1.13.7. Ser compatível com dispositivos de rede: Cisco, Extreme, HP, 3com, DELL, NVIDIA Mellanox.
3.1.13.8. Ser compatível com aplicações: Apache Tomcat, Apache HTTP Server.
3.1.13.9. Ser compatível com aplicações Windows: contas de serviço e pools de aplicações do IIS
3.1.13.10. Ser compatível com serviços de Diretórios: AD, LDAP
3.1.13.11. Ser compatível com ambientes virtuais: VMware e Hyper-V;
3.1.13.12. Ser compatível com Storages: DELL/EMC, Huawei e IBM;
3.1.13.13. Ser disponibilizada um SDK (Software Development Kit) ou API (Application Programming Interface) que pode ser configurado para permitir que aplicações clientes possam:
3.1.13.14. Solicitar credenciais e dispositivos;
3.1.13.15. Cadastro e alteração credenciais e dispositivos;
3.1.13.16. Solicitar chaves SSH;
3.1.13.17. Ser compatível com aplicações em nuvem da Microsoft Azure.

3.1.14. **Cofre de Informações privilegiadas**

3.1.14.1. A solução deve armazenar senhas para aplicações e serviços online.
3.1.14.2. A solução deve possuir registro de acesso a informações privilegiadas.
3.1.14.3. A solução deve ter a possibilidade de compartilhar informações com outros usuários.
3.1.14.4. A solução deve possuir APIs para gerenciar itens do cofre.
3.1.14.5. A solução deve guardar registros para fins de auditoria e coleta de evidências de credenciais alteradas, para possível restauração dos mesmos.
3.1.14.6. A solução deve oferecer importação em lote de senhas, e chaves.
3.1.14.7. A solução deve possuir um dashboard administrativo com opções de ambiente.

3.1.15. **Fluxos de Aprovação**

3.1.15.1. A solução deverá ser flexível no processo de aprovação para o acesso a contas privilegiadas (acessos pré-aprovados, acessos com aprovação única e acessos com aprovações multiníveis).
3.1.15.2. A solução deverá permitir a configuração de fluxos de aprovação diferenciados por criticidade e características da conta, como contras privilegiadas e contas de uso por terceiros.
3.1.15.3. A solução deverá permitir a alteração, por parte do aprovador, do período de acesso solicitado por um usuário.
3.1.15.4. Caso uma solicitação de acesso seja aprovada, a sessão e o privilégio concedido deverão expirar automaticamente ao final do período autorizado.
3.1.15.5. O acesso ao fluxo de solicitação e aprovação deve ser possível de ser realizado de forma remota e segura.
3.1.15.6. A solução deve possuir função para revogar todos os acessos de uma pessoa de maneira imediata.
3.1.15.7. A solução deve oferecer um campo para que seja inserido um número identificador de demanda ou mudança ao qual o acesso estará associado.
3.1.15.8. A solução deve oferecer interface para usuários e auditores, provendo mecanismos de controle de acesso flexíveis para criar visões/grupos personalizados de dispositivos gerenciados e contas privilegiadas.

3.1.16. **Notificações e Alertas**

3.1.16.1. As notificações ou alertas emitidos pela solução devem ser customizáveis.
3.1.16.2. Envio de alerta ao Microsoft Sentinel (SIEM) de senhas que não estejam iguais ao cofre.
3.1.16.3. A solução deve ser configurável para registrar eventos de sistema e enviar alertas por e-mail, SNMP e/ou dashboard da própria solução, com possibilidade de exportação dos logs e relatórios, contemplando ao menos um dos seguintes serviços:
3.1.16.3.1. Caso serviços essenciais estejam parados;
3.1.16.3.2. Caso atinja o limite de processamento da CPU;
3.1.16.3.3. Caso atinja o limite de processamento da memória;
3.1.16.3.4. Caso atinja o limite de capacidade do armazenamento de dados.
3.1.16.4. A solução deve ser capaz de notificar, via e-mail, novas solicitações de acesso para as pessoas responsáveis pela aprovação.
3.1.16.5. A solução deve ser capaz de notificar ao solicitante de um acesso, via e-mail, acessos que foram ou não aprovados.
3.1.16.6. As notificações devem ser parametrizáveis, de modo que o administrador da solução possa habilitar/desabilitar individualmente as notificações.

3.1.17. **Relatórios e Dashboards**

3.1.17.1. A solução deve permitir que os módulos de visualização de sessões e geração de relatórios apresentem o número de registros localizados e paginação de resultados para cada pesquisa realizada.
3.1.17.2. A solução deve permitir a geração de relatórios de todos os usuários cadastrados na aplicação, e seus respectivos papéis.
3.1.17.3. A solução deve permitir a geração de relatórios de contas de usuários privilegiados monitoradas pela ferramenta.
3.1.17.4. A solução deve possuir mecanismos para geração de relatórios a respeito das contas privilegiadas, tais como listas de ativos e suas contas gerenciadas, requisições de acesso a contas privilegiadas submetidas a aprovação, aprovadas ou rejeitadas e histórico de utilização das contas privilegiadas.
3.1.17.5. Os relatórios devem estar disponíveis na dashboard da solução, com a possibilidade de exportação, para um dos seguintes formatos: PDF, XLSX e/ou CSV.
3.1.17.6. A solução deve registrar atividades administrativas, como modificações de políticas e contas.
3.1.17.7. A solução deve relatar a data do último logout de cada conta privilegiada, a fim de identificar contas possivelmente não mais usadas.
3.1.17.8. Fornecer uma lista de contas de usuário habilitadas as quais senha não foi alterada em mais de 30 dias.
3.1.17.9. Conter um histórico detalhado de todas as alterações de segurança de senha feitas nos dispositivos por qualquer usuário.
3.1.17.10. Listar todas as contas gerenciadas pela solução juntamente com os detalhes da idade da senha.
3.1.17.11. Listar detalhes de conta de usuário de ativos, filtrados por localização, status, associação de grupo e entre outros.
3.1.17.12. Fornecer uma visualização transacional detalhada de atividades de sessão da solução.
3.1.17.13. Fornecer lista com detalhes da atividade de liberação de senha da solução.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.1.17.14. Fornecer os detalhes da atividade de atualização de senha da solução
3.1.17.15. Fornecer os detalhes das próximas atualizações de senha programadas.
3.1.17.16. Fornecer uma lista detalhada de quais sistemas estão usando uma conta de serviço da solução para iniciar um ou mais serviços.
3.1.17.17. Histórico de utilização da credencial: A solução deve armazenar o histórico de utilização das credenciais, assim como qualquer outro tipo de ação associada a seu uso como gerenciamento remoto, finalização da sessão por administrador, etc. O histórico pode ser visualizado na própria solução ou através da geração de relatórios de auditoria.
3.1.17.18. Relatórios de operação com lista de usuários, equipamentos e credenciais cadastradas.
3.1.17.19. Relatórios de Auditoria.
3.1.17.20. Exportação para Excel e/ou “CSV”.
3.1.17.21. Dashboard de utilização.
3.1.17.22. Dashboard de conexões.
3.1.17.23. Dashboard de utilização de sessões.
3.1.17.24. Dashboard de sessão ativas de usuários.
3.1.17.25. A solução deve controlar o acesso aos relatórios se baseando nas permissões configuradas na solução.
3.1.17.26. Registrar cada acesso, incluindo os acessos via aplicação web para solicitações de senha, aprovações, checkouts, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas.
3.1.17.27. A solução deve fornecer dados ad-hoc agendados, relatórios em tempo real dos usuários, contas, configuração da solução e informações sobre os processos da solução.
3.1.17.28. A solução deve apresentar relatórios com visibilidade hierárquica, contendo listas e filtros de ordenação de tal forma que os usuários possam detalhar as informações e os recursos que desejam acessar.

3.1.18. **Logs e Auditoria**

3.1.18.1. A solução deverá permitir integração com ferramenta de SIEM de acordo com os padrões de mercado, por meio de provisionamento de informações ou envio automático de logs para servidores SYSLOG, aderente aos princípios da RFC 5424.
3.1.18.2. A solução deve possuir trilha de auditoria sobre a aplicação de regras para cada conta de acesso privilegiado.
3.1.18.3. A solução deve possibilitar o rastreamento de todas as ações realizadas nos sistemas gerenciados por meio das contas privilegiadas.
3.1.18.4. O sistema deve registrar todas as atividades executadas e disponibilizar os dados de auditoria a usuários com perfil adequado, como por exemplo perfil de Auditor.
3.1.18.5. A solução deve alertar ao usuário que a sessão está sendo gravada, podendo ter o banner de alerta pelo administrador da solução.
3.1.18.6. A solução deve prover mecanismo de busca de gravações registradas dos acessos nos ativos.
3.1.18.7. A solução deve permitir a busca por comandos específicos executados pelo usuário como em sessões SSH e Windows.

3.1.18.8. O mecanismo de gravação deve ser fornecido e desenvolvido como parte integrante da solução, não sendo aceitos programas de outros fabricantes que não o desenvolvedor da solução proposta.
3.1.18.9. A solução deve ser capaz de armazenar os vídeos das sessões em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências.
3.1.18.10. A solução deve otimizar o armazenamento dos vídeos gravados no appliance.
3.1.18.11. A solução deve ser capaz de registrar em vídeo a sessão do usuário, independentemente da forma de acesso.
3.1.18.12. A solução deve controlar o acesso as sessões gravadas, tanto como permissão, como registrando quem teve acesso.
3.1.18.13. A solução deve suportar a pesquisa dos comandos executados e vincula esses comandos aos quadros das sessões gravadas e armazenadas.
3.1.18.14. Expiração e expurgo das gravações de forma automática ou manual.
3.1.18.15. Possibilidade de armazenamento e exportação das gravações para locais fora do PAM (rede local ou nuvem).

3.1.19. **Autenticação**
3.1.19.1. A solução deverá possibilitar autenticação transparente no sistema-alvo, com início de sessão por meio da injeção direta de credenciais.
3.1.19.2. A solução deverá permitir autenticação multifator de usuário (MFA).
3.1.19.3. A solução deve integrar-se com soluções de autenticação de duplo fator compatíveis com o Microsoft Azure AD.
3.1.19.4. A solução deverá ser integrada a base de usuários com privilégios administrativos do Microsoft Active Directory e RADIUS para concessão de acesso a plataforma e a atribuição de perfis de acesso às funcionalidades do sistema.
3.1.19.5. Autenticação centralizada integrada com protocolo SAML;
3.1.19.6. Autenticação centralizada integrada com autenticação por certificado digital pessoal para usuários e administradores;
3.1.19.7. Deve possuir duplo fator de autenticação nativo para acesso web ou através de client;
3.1.19.8. A solução deverá ser capaz de bloquear usuários e sessões que estejam dentro das seguintes características de acesso:
3.1.19.9. Autenticação centralizada integrada com LDAP, LDAPS para MS AD com múltiplos DCs.

3.1.20. **Gestão de Usuários e Perfis**
3.1.20.1. Cadastro de usuários com informações de nome, e-mail e departamento, no mínimo.
3.1.20.2. Cadastro de perfis de usuários.
3.1.20.3. Segregação de funções por perfis de acesso.
3.1.20.4. Flexibilidade para criação de quaisquer perfis customizados, com diversas combinações de telas e funcionalidades de acordo com a necessidade do negócio, sem intervenção do fornecedor.
3.1.20.5. Criação de TAGs ou lançadores personalizados para definir dispositivos e credenciais;
3.1.20.6. Importação automática de contas de usuários do AD
3.1.20.7. Importação automática de contas de usuários do LDAP;
3.1.20.8. Gerenciamento de Grupos e Perfis de acesso integrados aos grupos de AD/LDAP.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.1.20.9. A solução deve permitir o gerenciamento e monitoramento de sessões estabelecidas via protocolos: HTTP, HTTPS, SSH e RDP, seja via Proxy ou Jump Server.
3.1.20.10. A solução deve permitir monitoramento em tempo real das sessões ou atividades dos usuários privilegiados, disponibilizada em interface centralizada (Dashboard).
3.1.20.11. A solução deve garantir a monitoração das atividades realizadas com contas de acesso privilegiado obtidas de forma emergencial (“break-glass”).
3.1.20.12. A solução deve possuir funcionalidade de gravação das sessões dos usuários privilegiados.
3.1.20.13. A gravação de sessão de usuário deve suportar a gravação contínua de toda a sessão em vídeo.
3.1.20.14. A gravação de sessão deve possibilitar o registro da iteração do mouse e teclado durante a sessão.
3.1.20.15. A solução deve suportar a gravação da sessão de usuários simultâneos. A quantidade máxima de sessões deve ser ilimitada, não tendo nenhuma limitação de software.
3.1.20.16. Gerenciamento e gravação de sessões
3.1.20.16.1. As gravações de sessão devem ser armazenadas em formato criptografado. É desejável que as gravações sejam armazenadas em formato compactado.
3.1.20.17. A solução não deverá depender da instalação de agentes para realizar a gravação de sessão.
3.1.20.18. Gravação de Vídeo das sessões realizadas através de webproxy ou proxy transparente em formato otimizado;
3.1.20.19. Gravação de comandos digitados em ambientes RDP e SSH;
3.1.20.20. Oferecer opção de assistir o vídeo de uma sessão realizada diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download;
3.1.20.21. Exportação de sessão em formato vídeo;
3.1.20.22. Busca de registro de sessão por usuário, sistema alvo, IP alvo, data e hora;
3.1.20.23. Busca por comandos e entradas de teclado digitados em plataforma Linux;
3.1.20.24. Busca de comandos e entradas de teclado em plataforma Windows;
3.1.20.25. Gravação de Logs de Input e Output de comandos, sem necessidade de agentes locais para gravação de sessão.
3.1.20.26. Armazenamento e consulta de logs que forneçam ao menos, as seguintes informações:
3.1.20.27. Identificação do usuário que realizou determinado acesso a um dispositivo;
3.1.20.28. Identificação de quem aprovou o acesso do usuário;
3.1.20.29. Data e hora do acesso realizado e das ações que o usuário realizou no dispositivo remoto.
3.1.20.30. Prover, ao menos, os seguintes filtros para a recuperação de logs:
3.1.20.30.1. Usuário;
3.1.20.30.2. Sistema-alvo acessado;
3.1.20.30.3. Tipo de atividade;
3.1.20.30.4. Intervalo de tempo.
3.1.20.31. Permitir o acompanhamento on-line de sessões remotas pelo administrador e desligamento da sessão remotamente;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.1.21. **PLATAFORMA**
3.1.21.1. Compatível com máquinas virtuais do VMware ESXi.
3.1.22. **IDIOMA**
3.1.22.1. Inglês (US) e/ou Português (Brasil);
3.1.23. **GARANTIA:**
3.1.23.1. Garantia e suporte técnico por 60 (sessenta) meses com as seguintes condições:
3.1.23.1.1. O serviço será prestado mediante Central de Atendimento 0800 ou por meio da internet, diretamente pelo fabricante das licenças, com a devida abertura de chamado técnico ilimitado.
3.1.23.1.2. O suporte deve ser prestado em regime 24x7 (vinte e quatro horas em sete dias por semana) de acordo com a seguinte classificação:
3.1.23.1.2.1. Severidade 1: O SLA para iniciar o atendimento será de no máximo 60 (sessenta) minutos para casos que afetem criticamente o uso do produto em ambiente de produção, como perda de registros de auditoria ou quando a solução estiver inoperante, a partir do início do atendimento.
3.1.23.1.2.2. Severidade 2: O SLA para iniciar o atendimento será de no máximo 4 (quatro) horas em dias úteis para casos que a solução se encontre em capacidade reduzida ou limitada incluindo impactos significativos em partes de operações de negócio e produtividade, ou onde a solução encontre-se exposta a potencial perda ou interrupção do serviço, a partir do início do atendimento.
3.1.23.1.2.3. Severidade 3: O SLA para iniciar o atendimento será de no máximo 08 horas em dias úteis para casos que a solução se encontre com perda parcial ou situação não crítica, permitindo que as operações de negócio continuem funcionando, a partir do início do atendimento.
3.1.23.1.2.4. Severidade 4: O SLA para iniciar o atendimento será de no máximo 01 dia para os demais casos, a partir do início do atendimento.
3.1.23.1.3. O vencedor do certame licitatório deverá apresentar a comprovação da sua contratação com o FABRICANTE da aquisição de pacote de garantia do fabricante para o usuário final de acordo com o nível de serviço citado acima.
3.1.23.1.4. É condição para o pagamento, a devida confirmação da disponibilidade no portal de suporte do fabricante e permissão para abertura de chamados e a comprovação de documento que estabeleça o prazo do serviço de suporte técnico para a solução adquirida.
3.1.24. **REQUISITOS DE CAPACITAÇÃO**
3.1.24.1. Apresentar no mínimo 2 atestados de capacidade técnica, referentes aos últimos 12 meses, para comprovação de fornecimento de solução de Gerenciamento de Acesso Privilegiado, fornecido por pessoa jurídica de direito público/privado, que comprove ter a CONTRATANTE prestado fornecimento, serviço de instalação ou manutenção de solução de contratada ou similar a exigida neste termo.
3.1.24.2. No caso de atestados emitidos por empresas privadas, não serão válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa LICITANTE. São consideradas como pertencentes

ao mesmo grupo empresarial as empresas controladas ou controladoras da empresa LICITANTE, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente ou empresa licitante.

3.1.24.3. Os atestados apresentados devem apresentar, ao menos, 50% do quantitativo pedido na descrição de licenças da Solução de Acessos Privilegiados.

3.1.24.4. O(s) atestado(s) apresentado(s) deverá(ão) conter no mínimo o CNPJ e endereço da entidade emitente, além de conter a data de emissão, o nome, função e telefone do responsável, e a qualidade do que foi executado.

3.1.24.5. A CONTRATANTE poderá apresentar tantos atestados quanto forem necessários para a comprovação dos quantitativos exigidos neste Termo de Referência.

3.1.24.6. Deverá apresentar comprovação emitida pelo fabricante da Solução para este certame, informando que a Contratada está apta e autorizada a comercializar os produtos e serviços objeto do Contrato.

3.1.25. **REQUISITOS DE FORMAÇÃO DE EQUIPE E EXPERIÊNCIA PROFISSIONAL**

3.1.25.1. O projeto deverá ser composto por uma equipe técnica liderado por um Gestor de Projeto da CONTRATADA, que deverá interagir com os representantes técnicos da CONTRATANTE.

3.1.25.2. Os serviços deverão ser realizados por técnicos qualificados e certificados pelo fabricante dos softwares da solução ofertada.

3.1.26. **MODELO DE EXECUÇÃO DO OBJETO:**

3.1.26.1. SUBCONTRATAÇÃO

3.1.26.1.1. É vedado à CONTRATADA transferir o objeto da prestação de serviços deste Termo de Referência por subcontratação

3.2. SERVIÇOS

3.2.1. **SERVIÇO DE TREINAMENTO**

3.2.1.1. A execução do treinamento será definida em uma reunião de kickoff, onde as partes acordarão sobre o início, prazo, e datas do treinamento. OS detalhes serão estabelecidos considerando as agendas dos participantes. Tudo será discutido, acordado e documentado em ATA, garantindo clareza e comprometimento mútuo para o sucesso do treinamento.

3.2.1.2. O treinamento deverá ser ministrado abrangendo teoria e prática de implantação, configuração, administração e solução de problemas e assuntos teóricos relacionados a todos os itens, bem como todas as funcionalidades disponíveis da solução ofertada.

3.2.1.3. O treinamento deve ser composto por curso oficial da fabricante abrangendo conteúdo teórico e prático, abordando todas as funcionalidades da ferramenta.

3.2.1.4. Deve tratar, no mínimo, as seguintes abordagens:

3.2.1.4.1. Apresentação da arquitetura da solução e dos conceitos fundamentais;

3.2.1.4.2. Instalação da solução;

3.2.1.4.3. Configuração inicial;

3.2.1.4.4. Configuração de interface;

3.2.1.4.5. Identificação de aplicações;

3.2.1.4.6. Administração da Solução;

3.2.1.4.7. Gerenciamento de senhas

3.2.1.4.8. Rotação de senhas

3.2.1.4.9. Controle de Acesso
3.2.1.4.10. Integração e compatibilidade
3.2.1.4.11. Cadastro de Ativos
3.2.1.4.12. Cofre de Informações privilegiadas
3.2.1.4.13. Fluxos de Aprovação
3.2.1.4.14. Notificações e Alertas
3.2.1.4.15. Relatórios e Dashboards
3.2.1.4.16. Análise de Comportamento
3.2.1.4.17. Logs e Auditoria
3.2.1.4.18. Autenticação
3.2.1.4.19. Gestão de Usuários e Perfis
3.2.1.4.20. Gerenciamento e gravação de sessões
3.2.1.4.21. Demais assuntos pertinentes a solução ofertada.
3.2.1.4.22. O treinamento deve ser ministrado com instrutores certificados pelo fabricante da solução.

3.2.1.5. O treinamento deve ser realizado no período de segunda a sexta-feira, em dias úteis, entre 8 (oito) horas e 18 (dezoito) horas e não poderá exceder o máximo de 8 (oito) horas diárias.

3.2.1.6. O treinamento poderá ser realizado na modalidade Ensino à Distância (EAD).

3.2.1.7. Na realização do treinamento em modalidade presencial, em nenhuma hipótese deverá existir custos adicionais ao CONTRATANTE para a realização do treinamento.

3.2.1.8. O fornecedor deve determinar a modalidade (EAD ou presencial) do treinamento e deverá fornecer toda a infraestrutura necessária para realização do treinamento. Recursos tais como instrutor, lanche, material, equipamentos, entre outros não terão ônus adicional para a CONTRATANTE.

3.2.1.9. A critério do contratante, o fornecedor poderá fornecer vouchers para realização de treinamento na solução adquirida a ser realizado, de forma presencial, nas instalações do fabricante ou de parceiro autorizado. Nesta hipótese, se a localização do centro de treinamento for fora da cidade de Porto Alegre, todas as despesas de deslocamento, hospedagem e alimentação dos alunos serão de responsabilidade do CONTRATANTE.

3.2.1.10. O treinamento deve ser ofertado em português.

3.2.1.11. O material didático impresso deve ser oficial, sendo uma unidade para cada dos participantes.

3.2.1.12. O treinamento deverá possuir carga horária mínima de 24 horas, podendo ser ampliada conforme a necessidade de operação da solução pelo CONTRATANTE e em quantos módulos forem necessários, de acordo com o treinamento oficial do fabricante da Solução de PAM.

3.2.1.13. Deve ser fornecido certificado de participação para cada participante a critério do contratante. O certificado de conclusão do curso deve descrever ao menos o título do curso, ter o nome completo do participante, informar a carga horária, o nome do instrutor, local e data da realização do curso.

3.2.1.14. O treinamento deverá ser ministrado para no mínimo 6 (seis) integrantes da equipe do contratante ou de seus subcontratados a seu critério.

3.2.1.15. Os cursos deverão ser ministrados antes da instalação da solução em definitivo.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.2.1.16. O conteúdo teórico dos treinamentos deve ficar disponível para os participantes para pesquisas futuras, após a conclusão do curso.

3.2.2. **SERVIÇO DE IMPLANTAÇÃO**

3.2.2.1. Os Serviços de Implantação compreendem a metodologia de trabalho para o planejamento, instalação, bem como a disposição adicional de horas técnicas para adequação da Solução de PAM ao uso da CONTRATANTE.

3.2.2.2. **SERVIÇO DE INSTALAÇÃO:**

3.2.2.2.1. Os serviços de instalação e configuração deverão ser prestados por técnicos certificados pelo fabricante da solução.

3.2.2.2.2. Deve ser fornecido juntamente com a solução os endereços eletrônicos para acesso às documentações técnicas, contendo todas as informações sobre os produtos ofertados com as instruções para instalação, configuração e operação, preferencialmente em português (Brasil), ou ser escritos em língua inglesa.

3.2.2.2.3. Toda a implantação e configurações da solução devem serem realizadas de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada.

3.2.2.2.4. Serviço de Verificação da Saúde da Solução (Testes)

3.2.2.2.5. O plano de testes apresentado pela CONTRATADA deverá ser executado e homologado.

3.2.2.2.6. Após a homologação da instalação e operação da solução em regime produtivo (ongoing), deve ser disponibilizado, de forma presencial no contratante, um técnico especializado para acompanhar a equipe técnica de sustentação na execução das principais tarefas administrativas da operação diária, atuando em esclarecimentos, ajustes e eventuais correções, durante 5 (cinco) dias úteis (operação assistida).

3.2.2.2.7. Deve ser realizada a transferência de conhecimento sobre a tecnologia durante o período de operação assistida sobre a solução no ambiente do contratante, para no mínimo para 3 (três) profissionais a critério do contratante (Hands-On).

3.2.2.2.8. Manutenção de Sigilo e Normas de Segurança

3.2.2.2.9. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

3.2.2.2.10. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXOS B.

3.2.2.2.11. Requisitos de Segurança e Privacidade

3.2.2.2.12. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.2.2.2.13. A CONTRATADA deverá assinar Termo de Sigilo/Confidencialidade obrigando-se a não realizar, promover, incentivar a divulgação de qualquer dado ou informação do ambiente computacional do CONTRATANTE, bem como dos dados ou informações contidas nele sem a prévia autorização;

3.2.2.2.14. Obedecer às normas internas do CONTRATANTE, relativas à segurança, à identificação, ao trânsito e à permanência de pessoas em suas dependências;

3.2.2.2.15. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, de todos os dados ou informações do CONTRATANTE ou suas representações obtidas em função da prestação do objeto contratado, além de qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato, devendo orientar seus profissionais nesse sentido;

3.2.2.2.16. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas:

3.2.2.2.16.1. À política de segurança adotada pelo CONTRATANTE;

3.2.2.2.16.2. Às instruções normativas vigentes da CONTRATANTE;

3.2.2.2.16.3. Às configurações de software decorrentes;

3.2.2.2.16.4. Ao processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos;

3.2.2.2.16.5. A quaisquer dados e informações armazenadas em sistemas do CONTRATANTE.

3.2.2.3. **METODOLOGIA DE TRABALHO:**

3.2.2.3.1. Prazo máximo para Instalação e configuração (implementação) da solução será de 60 (sessenta) dias corridos contados a partir da disponibilização dos hipervisores, devendo ser realizada conforme horário para prestação do serviço definido pelo CONTRATANTE.

3.2.2.3.2. Os serviços devem ser planejados em conjunto com o contratante, prevendo o menor tempo de parada possível (downtime) dos serviços durante sua execução. A critério do contratante este tempo de parada pode exigir tarefas e ações de mitigação deste tempo.

3.2.2.3.3. Deverá ser fornecido Relatórios de Pré-Requisitos de Instalação e Operação dos Produtos, contendo, por produto, informação de todos os seus pré-requisitos instalação e operação, a citar: todas conexões lógicas e configuração necessárias para interligação da solução com o ambiente proposto pela CONTRATANTE;

3.2.2.3.4. 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;

3.2.2.3.5. 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 pela SEFAZ-RS;

3.2.2.3.6. Para finalizar fase de instalação e ter início a fase de configuração, a CONTRATADA deverá apresentar os seguintes documentos:
3.2.2.3.7. Plano de Configuração:
3.2.2.3.8. Diagrama de interconexão da solução;
3.2.2.3.9. Projeto lógico de configuração;
3.2.2.3.10. Configuração da solução;
3.2.2.3.11. Após instalação física da solução, deverão ser realizadas as configurações avançadas, que irão efetivamente integrar a nova solução ao ambiente computacional do CONTRATANTE;
3.2.2.3.12. 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;
3.2.2.3.13. As atividades de instalação dos equipamentos deverão ocorrer, preferencialmente, em dias úteis, no período estabelecido nesse Termo de Referência para prestação dos serviços nos respectivos locais;
3.2.2.3.14. Caso a configuração possa provocar indisponibilidade nos serviços, a instalação poderá ocorrer em horário noturno e/ou fim de semana, a critério do CONTRATANTE;
3.2.2.3.15. Os procedimentos envolvidos nos processos de configuração deverão ser previamente aprovados pelo CONTRATANTE;
3.2.2.3.16. Após a configurações deverá ser agendado a execução do plano de testes para demonstrar efetividade das configurações realizadas e funcionamento de cada característica da Solução adquirida.

3.2.2.4. **REQUISITOS DA IMPLANTAÇÃO:**

3.2.2.4.1. A Solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management - PAM) para controle da segurança de identidade deverá operar em Alta Disponibilidade (High Availability – HA).
3.2.2.4.2. A Solução deverá funcionar sobre tecnologias de virtualização, atendendo as seguintes especificações:
3.2.2.4.3. Extrair o melhor proveito dos hardwares virtualizados disponibilizados pela CONTRATADA para implementação, contribuindo com a redução no consumo de energia elétrica, diminuição na geração de lixo eletrônico e menor emissão de carbono.
3.2.2.4.4. Caso o banco de dados e/ou o Sistema Operacional utilizados pela Solução sejam de terceiros (exemplo: Oracle Database / MSSQL ou Windows Server / Red Hat Enterprise Linux), a solução deverá ser entregue com as licenças de software e garantia compatíveis com a solução a garantia da solução ofertada;
3.2.2.4.5. A solução deverá operar como um Cluster, incluindo seu sistema gerenciador de banco de dados.
3.2.2.4.6. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.
3.2.2.4.7. Para o caso acima, a empresa CONTRATADA deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação, sem custos adicionais para a CONTRATANTE.
3.2.2.4.8. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é

vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

3.2.2.4.9. A validação dos certificados e certificações fornecidos pelo fabricante deve ser realizada antes da assinatura do contrato. Adicionalmente, é necessário apresentar o Termo de Compromisso e de Manutenção de Sigilo por parte de todos os participantes envolvidos no projeto.

3.2.2.5. **ARQUITETURA DE IMPLANTAÇÃO:**

3.2.2.5.1. A solução deve ser licenciada e implantada em 01 (uma) localidade com suporte a alta disponilibidade;

3.2.2.5.2. Para que a solução continue funcionando localmente mesmo com a falha de um nó de cada elemento, no mínimo os seguintes elementos devem ser instalados em regime de alta disponibilidade:

3.2.2.5.3. Cofre de senhas (entendido como o elemento da solução que controla as credenciais de acesso, incluindo a interface de acesso dos usuários à solução);

3.2.2.5.4. Gateway/Proxy de Sessão (elemento que provê e controla o acesso privilegiado monitorado aos ativos de TI);

3.2.2.5.5. A solução deve replicar as configurações e registros de auditoria nos 02 (dois) nós, de modo que, no evento de falha total de seus elementos instalados em um nó, a solução continue disponível através do segundo nó;

3.2.2.5.6. Devem ser fornecidas pela CONTRATADA, no quantitativo necessário para atender aos requisitos de arquitetura e alta disponibilidade apresentados, com todas as licenças válidas, com garantia igual ao do objeto desta contratação e sem custos adicionais para a CONTRATANTE.

3.2.2.5.7. O modelo mínimo de funcionamento e tolerância a falhas a ser implantado deve ser do tipo ativo-ativo.

3.2.3. **SERVIÇO EM HORAS TÉCNICAS:**

3.2.3.1. A CONTRATADA deverá dispor de um banco de horas técnicas, num total de 200 (duzentas) horas adicionais ao fim da implementação, para serem utilizados de acordo com a demanda, em horário comercial, por iniciativa exclusiva do CONTRATANTE.

3.2.3.2. As horas serão consumidas ao longo do período de validade do contrato, através da emissão de Ordem de Serviço, informando o prazo para início de execução das atividades.

3.2.3.3. Todos os serviços solicitados serão referentes ao objeto deste Termo de Referência e outros componentes da solução, que poderão ser utilizadas para fins de projetos ou implementações que não façam parte do escopo deste edital.

3.2.3.4. Quando um serviço for demandando, este deve ser medido pela CONTRATADA e validado pelo contratante. Após esta validação, esse serviço será catalogado com a sua respectiva quantidade de Horas Técnicas, para ser utilizado como parâmetro de mensuração em novas demandas.

3.2.3.5. Após definido o tamanho do serviço em Horas Técnicas, o esforço empregado na execução da demanda é responsabilidade da CONTRATADA, ou seja, qualquer fator (por exemplo: atraso) que não tenha sido causado pela mudança do escopo do que foi demandado, não acarretará ônus de qualquer tipo para o CONTRATANTE.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

3.2.3.6. Os serviços serão executados presencialmente nas dependências do CONTRATANTE, os quais poderão ter exceções autorizadas a seu critério.

3.2.4. **LOCAIS DA PRESTAÇÃO DO SERVIÇO:**

3.2.4.1. Os serviços serão prestados nos seguintes endereços:

3.2.4.2. Prédio sede da Cia de Processamento de Dados do RS – PROCERGS. Praça dos Açorianos, s/n. Porto Alegre RS.

3.2.4.3. Prédio Sede da Secretaria da Fazenda do RS – SEFAZ-RS. Av. Mauá, 1155, Porto Alegre RS.

3.2.5. **HORÁRIOS DA PRESTAÇÃO DOS SERVIÇOS:**

3.2.5.1. Fica definido o horário das 09:00 às 17:00 nos locais para prestação de serviços.

3.2.5.2. A CONTRATANTE poderá considerar alterar os horários previamente definido através de estabelecimento de acordo com a CONTRATADA

4. DESCRIÇÃO DA SOLUÇÃO:

4.1. A solução de Gerenciamento de Acesso Privilegiado (Privileged Access Management - PAM) é um software focado no controle da segurança de identidade que ajuda a proteger as organizações contra ameaças cibernéticas ao monitorar, detectar e impedir o acesso privilegiado não autorizado a recursos críticos.

4.2. A solução deverá ser capaz de operar em alta disponibilidade, sendo seu fornecimento composto basicamente por:

4.3. Solução de Gerenciamento de Acesso Privilegiado, com fornecimento de Licenças por subscrição, pelo período de 60 meses;

4.4. Serviço de Treinamento e Implantação da Solução de Gerenciamento de Acesso Privilegiado;

4.5. Conforme Especificações Técnicas, a solução deverá ser compatível com o ambiente existente na SEFAZ, integrando-se aos ambientes de produção e desenvolvimento da Secretaria. Além disso, deverá estar totalmente integrada às soluções de segurança existentes.

5. MODELO DE GESTÃO DO CONTRATO:

5.1. Solução de Gerenciamento de Acesso Privilegiado, com fornecimento de Licenças por subscrição, pelo período de 60 meses O contratado é obrigado a submeter, mensalmente, um relatório detalhado de todas as ordens de serviço geradas durante o período. Este documento deve incluir informações essenciais como data de abertura, fechamento, grau de criticidade, e o nome do responsável pela abertura de cada ordem.

5.1.1. A solução de gerenciamento será considerada definitivamente recebida apenas após a finalização do serviço de Implantação, sendo indispensável a apresentação do relatório descrito no item 5.2.2

5.2. Serviço de Treinamento e Implantação da Solução de Gerenciamento de Acesso Privilegiado.

5.2.1. Treinamento: Após a conclusão do treinamento, será necessário apresentar um relatório de encerramento que detalhe as datas de realização, carga horária total, identificação do responsável pelo treinamento, cópia do material didático utilizado, e a lista de participantes. Este documento visa documentar o cumprimento e a eficácia do treinamento oferecido.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

5.2.2. Implantação: Deve-se entregar um relatório resumido que destaque os principais marcos alcançados durante a fase de implantação, incluindo o cronograma de execução, os desafios encontrados e as soluções adotadas, culminando com o relatório final de implantação. Este relatório deve alinhar-se com os requisitos especificados no item 3.2.2.1.1, garantindo que todos os aspectos da implantação foram devidamente executados e documentados

5.3. Serviço de Horas Técnicas:

5.3.1. Após a implantação será apresentado recibo do quantitativo de horas técnicas disponíveis para consumo durante a validade do contrato.

6. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO:

6.1. O processo de medição e pagamento será estruturado em duas fases principais:

6.1.1. Na primeira fase, um Atestado de Recebimento Provisório será emitido, condicionado à entrega e avaliação do relatório final de implantação e recibo do quantitativo de horas técnicas disponibilizadas pelo contratante. Esta etapa assegura que todos os requisitos e funcionalidades acordados foram adequadamente implementados e estão operacionais.

6.1.2. Após um período de validação de até 7 dias, destinado à verificação e testes finais de todo o escopo de trabalho realizado, o Atestado de Recebimento Definitivo será liberado.

6.2. O pagamento, por sua vez, será efetuado em uma parcela única, subsequente à emissão do Atestado de Recebimento Definitivo.

6.3. O serviço de treinamento deverá receber Atestados de recebimentos próprios, condicionado à entrega do Relatório de Encerramento.

6.4. Cronograma de pagamento:

Item	Até 90 dias a contar da Ordem de início	Até 120 dias a contar da Ordem de Início
Solução de Gerenciamento	100%	
Serviço de Implantação	100%	
Serviço de Treinamento		100%
Serviço de Horas Técnicas	100%	
% Contrato Pago	**97%**	**100%**

6.4.1. A execução do cronograma de pagamento depende de serem respeitados os prazos estabelecidos para a execução dos serviços.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

7. ADEQUAÇÃO ORÇAMENTÁRIA:

7.1. Esta aquisição será custeada com o Recurso 0377, Projeto 5735 – PROFISCO II.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

ANEXO A
PREMISSAS DO PROJETO

1. Requisitos do Negócio

Aquisição de Solução de Gerenciamento de Acesso Privilegiado (*Privileged Access Management* - PAM) para controle da segurança de identidade que contribui com a proteção contra ameaças cibernéticas ao monitorar, detectar e impedir o acesso privilegiado não autorizado a recursos.

A solução deve atender as seguintes premissas mínimas:

- Estar licenciada para uso de:
  - Usuários Nominais: 140
  - Usuários Administrativos: 10
  - Usuários de Serviços: 10
  - Ativos de Rede: 10
  - Estações de Trabalho: 10
  - Servidores Windows: 345
  - Servidores Linux: 70
- Solução deve ser capaz de operar em alta disponibilidade.
- Deve suportar login de ao menos 2 Usuários Administrativos em serviço de nuvem Microsoft Entra (Azure).
- A solução não deve exigir plugins de navegadores (Flash, Java, Extensões, entre outros) para qualquer função de acesso, inicialização, revisão, administração ou gerenciamento.
- Possuir cofre de senhas para o gerenciamento de permissões de acesso a informações por níveis hierárquicos ou funções.
- Suportar a proteção do ambiente DevOps com segurança de senha integrada ao deploy.
- Permitir acesso remoto seguro usando gateways criptografados em vez de senhas.

Suportar autenticação multifator (MFA) e logon único (SSO).

- Deverá permitir a configuração e definição de fluxos de aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas.
- Deverá permitir a configuração de fluxo de aprovação de acordo com a criticidade e características da conta (como de acesso emergencial ou de terceiros), e aprovação de pelo menos um responsável.
- Fornecer acesso just-in-time a recursos críticos.
- Monitorar sessões privilegiadas através dos protocolos SSH e RDP, permitindo gravação da sessão e de seus comandos executados para dar suporte a auditorias investigativas.
  - Deverá permitir a busca por comandos em gravações, bem como possuir uma linha do tempo para navegação em seu conteúdo.
- Ser compatível com as soluções de Rede, NGFW e Nuvem da SEFAZ-RS.
- Suportar a arquitetura “tierizada” da SEFAZ-RS.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

- Executar em máquinas virtuais compatíveis com hipervisor VMware.
- Incluir serviço de Instalação, Configuração e Integração com os Sistemas da SEFAZ-RS, incluindo os Sistemas Operacionais Windows e Linux.
- Gerar relatórios sobre acesso e atividade de usuários privilegiados.
- Treinamento abrangendo todas as funcionalidades da solução a ser adquirida.
- Dispor de banco de horas técnicas de 200 (duzentas) horas, para serem utilizados de acordo com a demanda de implementações adicionais.
- Garantia e Suporte técnico especializado mensal por 60 meses para Software.

2. *Requisitos da Arquitetura Tecnológica*

A Solução de Gerenciamento de Acesso Privilegiado (*Privileged Access Management* - PAM) para controle da segurança de identidade deverá operar em Alta Disponibilidade (*High Availability* – HA) sobre a estrutura de virtualização da SEFAZ-RS.

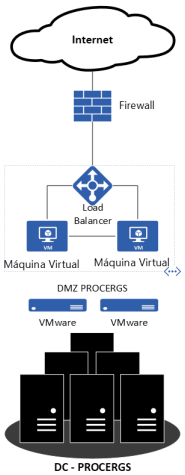

Figura 1 – Arquitetura lógica para Solução de PAM da SEFAZ-RS

A implementação da Solução será de responsabilidade da CONTRATADA e deverá executar sobre sistemas operacionais virtualizados, devidamente instalados, configurados e integrados à rede existente, operando perfeitamente, utilizando-se de boas práticas de segurança recomendas pelo fabricante dos softwares utilizados.

Todo licenciamento adicional para operação em Alta Disponibilidade de máquinas virtuais da Solução deverá ser custeado pela CONTRATADA.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

ANEXO B
TERMO DE COMPROMISSO E MANUTENÇÃO DO SIGILO

A Secretaria da Fazenda do Estado do Rio Grande do Sul – SEFAZ/RS, situada na Av. Mauá, 1155 ou Rua Siqueira Campos, 1044 | Porto Alegre / RS, de um lado doravante denominada CONTRATANTE, e de outro lado, a empresa _____, inscrita no CNPJ sob o número _____, com Sede no endereço: _____, CEP: _____, doravante denominada CONTRATADA; CONSIDERANDO que, em razão do CONTRATO Nº XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações

sigilosas da CONTRATANTE; CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL.

Cláusula Segunda – DAS INFORMAÇÕES SIGILOSAS

Será considerada como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, independente de conter ou não a chancela de classificação, em linguagem computacional em qualquer nível, qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter conhecimento em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Terceira – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia de INFORMAÇÕES sem o consentimento formal e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção das INFORMAÇÕES da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Quinto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às INFORMAÇÕES.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor, desde a data de sua assinatura, mesmo após o término da execução do CONTRATO PRINCIPAL e suas respectivas prorrogações.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civis e criminais, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tais como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, Termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras Pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, será incorporado a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessária a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o Juízo Federal, Seção Judiciária do Distrito Federal, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas às condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

Porto Alegre/RS, ____ de _____de 20___.

De acordo.

_____

Nome do preposto:

Cargo:

Empresa: